NETGEAR®

ProSAFE Wireless Controller WC9500

Reference Manual

May, 2013
202-11224-02

350 East Plumeria Drive
San Jose, CA 95134
USA

Support

Thank you for selecting NETGEAR products.

After installing your device, locate the serial number on the label of your product and use it to register your product at *https://my.netgear.com*. You must register your product before you can use NETGEAR telephone support. NETGEAR recommends registering your product through the NETGEAR website. For product updates and web support, visit *http://support.netgear.com*.

Phone (US & Canada only): 1-888-NETGEAR.

Phone (Other Countries): Check the list of phone numbers at *http://support.netgear.com/general/contact/default.aspx.*

Trademarks

NETGEAR, the NETGEAR logo, and Connect with Innovation are trademarks and/or registered trademarks of NETGEAR, Inc. and/or its subsidiaries in the United States and/or other countries. Information is subject to change without notice. © NETGEAR, Inc. All rights reserved.

Revision History

Publication Part Number	Publish Date	Comments
202-11224-02	May 2013	Color correction and minor nontechnical edits
202-11224-01	April 2013	First publication

Contents

Chapter 1 Introduction

Key Features and Capabilities 9
Package Contents 11
Hardware Features 11
Front Panel Ports, Slots, and LEDs 11
Back Panel Features 13
Bottom Panel with Product Label 14
WC9500 Wireless Controller System Components 14
NETGEAR ProSAFE Access Points 15
What Can You Do with the WC9500 Wireless Controller? 16
Licenses 18
Maintenance and Support 18

Chapter 2 System Planning and Deployment Scenarios

Basic and Advanced Setting Concepts 20
Profile Group Concepts 21
Basic Profile 21
Advanced Profile 21
System Planning 23
Preinstallation Planning 23
Before You Configure a Wireless Controller 23
High-Level Configuration Examples 26
Single Controller Configuration with Basic Profile Group 26
Single Controller Configuration with Advanced Profile Groups 27
Management VLAN and Data VLAN Strategies 27
High-Level Deployment Scenarios 29
Scenario Example 1: Network with Single VLAN 29
Scenario Example 2: Advanced Network with VLANs and SSIDs 31
Scenario Example 3: Advanced Network 34

Chapter 3 Installation and Configuration Overview

Initial Set up and Log in 39
Web Management Interface Layout 41
Roadmap for Initial Configuration 42
Roadmap for Configuring Management of Your Wireless Network 43
Choose a Location for the Wireless Controller 45
Deploy the Wireless Controller 45

Chapter 4 Configure the System and Network Settings and Register the Licenses

Configure General Settings 47
Manage the Time Settings 48
IP and VLAN Settings 49
Management VLAN Concepts 49
Untagged VLAN Concepts 49
Configure the IP and VLAN Settings 49
Manage the DHCP Server 51
Register Your Licenses 54
Configure the License Server Settings 54
Register Your Licenses with the License Server 55
Manage Certificates 57
Configure Log, Syslog, Alarm Notification, and Email Settings 58
Configure Log Settings 58
Configure Syslog Settings 60
Configure Alarm Notification Settings 61
Configure the Email Notification Server 62

Chapter 5 Manage Security Profiles and Profile Groups

Wireless Security Profile Concepts 64
Small WLAN Networks 64
Larger WLAN Networks 65
Profile Naming Conventions 65
Considerations Before You Configure Profiles 65
Basic and Advanced Security Configuration Concepts 66
Configure Security Profiles for the Basic Profile Group 67
Configure Profiles in the Basic Profile Group 67
Edit and Remove Profiles in the Basic Profile Group 70
Configure Security Profiles for Advanced Profile Groups 71
Advanced Profile Groups 71
Configure Profiles in an Advanced Profile Group 73
Edit and Remove Profiles in an Advanced Profile Group 76
Network Authentication and Data Encryption Options 77
Manage MAC Authentication and MAC Authentication Groups 81
Guidelines for External MAC Authentication 81
Configure Basic Local MAC Authentication Settings 82
Configure Local MAC Authentication Groups 84
Manage Authentication Servers and Authentication Server Groups 85
Configure Basic Authentication Server Settings 86
Configure RADIUS Authentication Server Groups 88

Chapter 6 Discover and Manage Access Points

Access Point Discovery Guidelines 91
General Discovery Guidelines 91
Layer 3 Discovery Guidelines 91

Discover Access Points with the Discovery Wizard 92
Access Points in Factory Default State and Access Points in a Layer 2 Subnet 92
Access Points Installed and Working in Standalone Mode in Different Layer 3 Networks 96
Manage the Managed AP List 100
View the Managed AP List 100
Edit Access Point Information on the Managed AP List 101
Remove Access Points from the Managed AP List 104
Assign Access Points to Advanced Profile Groups 104

Chapter 7 Manage Rogue Access Points, Guest Network Access, and Users

Manage Rogue Access Points 108
Configure Basic Rogue Detection Settings. 108
Classify Rogue Access Points 109
Import a List of Known Access Points from a File 110
Manage Guest Network Access 111
Portal Concepts 111
Configure a Portal. 113
Manage Users, Accounts, and Passwords. 116
Add a Management User 116
Add a WiFi Client 118
Add a Captive Portal Account. 119
Add a Captive Portal User 120
Edit or Remove a User or Account 122
Export a List of Users or Accounts 123

Chapter 8 Configure Wireless and QoS Settings

Basic and Advanced Wireless and QoS Configuration Concepts 125
Configure the Radio 126
Configure the Radio for the Basic Profile Group. 126
Configure the Radio for an Advanced Profile Group 127
Configure Wireless Settings 128
Configure Wireless Settings for the Basic Profile Group 128
Override Channel and Transmission Power in the Basic Profile Group 131
Configure Wireless Settings for an Advanced Profile Group 133
Override Channel and Transmission Power in an Advanced Profile Group. 135
Configure Channels 137
Specify RF Management 140
WLAN Healing 140
RF Management for the Basic Profile Group 141
RF Management for an Advanced Profile Group 142
Configure QoS for Advanced Profile Groups 144
Configure Load Balancing 147
Configure Rate Limiting 148

Rate Limiting for the Basic Profile Group 149
Rate Limiting for an Advanced Profile Group 150

Chapter 9 Maintain the Wireless Controller and Access Points

Manage the Configuration File 152
Back Up the Configuration File 152
Restore the Configuration File 153
Upgrade the Firmware 153
Reboot or Reset the Wireless Controller 156
Manage Remote Access 157
Specify Session Time-Outs 159
View Alerts and Events and Save the Logs 159
Query the System Logs 159
View Alerts and Events 162
Manage Licenses 165
View Your Licenses 165
Retrieve Your Licenses 167
Reboot Access Points 167
Configure Multicast Firmware Upgrade for Access Points 168
Change the Multicast Firmware Upgrade Settings 169
Disable Multicast Firmware Upgrade 169

Chapter 10 Monitor the Wireless Network and Its Components

Common Tasks on the Monitoring Screens 172
Monitor the Wireless Controller 173
View the Wireless Controller Summary Screen 173
View Wireless Controller Usage 175
View Access Points Managed by the Wireless Controller 176
View Clients Managed by the Wireless Controller 180
View Neighboring Clients Detected by the Wireless Controller 184
View Neighboring Access Points Detected by the Wireless Controller 185
View Security Profiles Managed by the Wireless Controller 186
View DHCP Leases Provided by the Wireless Controller 187
View Captive Portal Users Managed by the Wireless Controller 188
Monitor the SSIDs 188
Monitor Local Clients 193

Chapter 11 Troubleshooting

Troubleshoot Basic Functioning 198
Power LED Is Not Lit 198
Status LED Never Turns Off 198
Ethernet Port LEDs Are Not Lit 199
Troubleshoot the Web Management Interface 199
Ethernet Cabling 199
IP Address Configuration 199
Internet Browser 200

Troubleshoot a TCP/IP Network Using the Ping Utility 200
Use the Reset Button to Restore Default Settings 201
Problems with Date and Time 202
Problems with Access Points 202
Discovery Problems 202
Connection Problems 203
Network Performance and Rogue Access Point Detection 203
Use the Diagnostic Tools on the Wireless Controller 203

Appendix A Factory Default Settings and Technical Specifications

Factory Default Settings 206
Technical Specifications 206
Password Requirements 207

Index

Introduction

1

This chapter includes the following sections:

- *Key Features and Capabilities*
- *Package Contents*
- *Hardware Features*
- *WC9500 Wireless Controller System Components*
- *NETGEAR ProSAFE Access Points*
- *What Can You Do with the WC9500 Wireless Controller?*
- *Licenses*
- *Maintenance and Support*

Note: For more information about the topics covered in this manual, visit the support website at *http://support.netgear.com*.

Note: Firmware updates with new features and bug fixes are made available from time to time on *downloadcenter.netgear.com*. Some products can regularly check the site and download new firmware, or you can check for and download new firmware manually. If the features or behavior of your product do not match what is described in this guide, you might need to update your firmware.

Key Features and Capabilities

The NETGEAR ProSAFE Wireless Controller WC9500 is a high-capacity, secured wireless controller intended for medium- to large-sized businesses, higher education institutions, hospitals, and hotels.

One wireless controller with the appropriate licenses can support up to 600 access points (APs) with up to 6,000 users. In a stacked configuration (supported in a future release), a stack of three wireless controllers can support up to 18,000 users. The wireless controller supports the IEEE 802.11a/b/g/n protocols and is 802.11ac ready for future deployment. The wireless controller allows you to manage your wireless network from a central point, implement security features centrally, support Layer 2 and Layer 3 fast roaming, configure a guest access captive portal, and support voice over Wi-Fi (VoWi-Fi).

The wireless controller is equipped with two 10 Gigabit Ethernet (10GbE) slots with standard SFP+ form factor for optional 10GBASE or 1000BASE GBICs. One RJ-45 Gigabit Ethernet port is available to access the wireless controller for management and for data and control communications between the wireless controller and the access points.

The wireless controller provides the following key features and capabilities:

- **Scalable architecture**
  - Purchased licenses in increments of 10, 50, or 100 access points allow for support of up to a maximum number of 200 access points on a single wireless controller. A single license for 200 access points is also available.
  - Support of 802.11a, 802.11b, 802.11g, and 802.11n modes. Ready for 802.11ac mode for future deployment.
  - Support for an extra power supply.
- **Autodiscovery of access points**
  - Autodiscovery of access points in the same Layer 2 domain.
  - Autodiscovery of access points across a Layer 3 domain.
  - Automatic download of wireless controller–based firmware to discovered access points that are added to the managed access point list.
- **Centralized management**
  - Single point of management for the entire wireless network.
  - Automatic firmware upgrade to all managed access points.
  - DHCP server for IP address provisioning.
  - Configurable management VLAN.
- **Security**
  - Identity-based security authentication with an external RADIUS or LDAP (Active Directory) server, or with an internal authentication server.
  - Support for nine access point profile groups[1] (one basic and eight advanced) on one wireless controller.

1. Number of profile groups depends on the access point model used with the wireless controller.

  - Up to eight profiles per access point profile group and eight profiles per radio (therefore, dual-band access points can support up to 16 profiles in one access point profile group).
  - Support for up to 144 profiles[1] on one wireless controller (eight profiles per access point group and eight groups per radio). Each profile supports settings for SSID, network authentication, data encryption, client separation, VLAN, MAC ACL, and wireless QoS.
  - Rogue access point detection and classification.
  - Guest access and captive portal access with cost and expiration accounting.
  - Scheduled wireless on/off times.
- **Wi-Fi Multimedia Quality of Service and advanced wireless features**
  - Wi-Fi Multimedia (WMM) support for video, audio, and voice over Wi-Fi (VoWi-Fi).
  - WMM power save option.
  - Automatic WLAN healing mechanism ensures seamless coverage for wireless users.
  - Layer 2 and Layer 3 seamless roaming support.
  - Local Layer 2 traffic switching and Layer 3 traffic processing at access point level for fast processing.
- **RF management**
  - Automatic control of access point transmit power and channel allocation to reduce interference.
  - Automatic load balancing of clients across access points.
  - Rate limiting per profile.
- **Monitoring and reporting**
  - Monitoring of the status of the network, wireless controllers, WLANs, and clients, and network usage statistics.
  - Specific health monitoring of access points.
  - Logging and emailing of system events, RF events, load-balancing events, and rate-limiting events.

For a list of all features and capabilities of the wireless controller, see the datasheet that you can download from *http://support.netgear.com/product/WC9500*.

1. Number of profiles depends on the access point model used with the wireless controller.

Package Contents

The ProSAFE Wireless Controller WC9500 product package contains the following items:

- ProSAFE Wireless Controller WC9500 appliance
- One AC power cable
- Rubber feet (four) with adhesive backing
- One rack-mount kit
- Straight-through Category 5 Ethernet cable
- *ProSAFE Wireless Controller WC9500 Installation Guide*

If any of the parts are incorrect, missing, or damaged, contact your NETGEAR dealer. Keep the carton, including the original packing materials, in case you need to return the product for repair.

Hardware Features

The front panel ports, slots, and LEDs, back panel components, and bottom label of the wireless controller are described in this section.

Front Panel Ports, Slots, and LEDs

The following figure shows the front panel of the wireless controller.

Figure 1. Front panel

The following figure shows a close-up of the left side of the front panel.

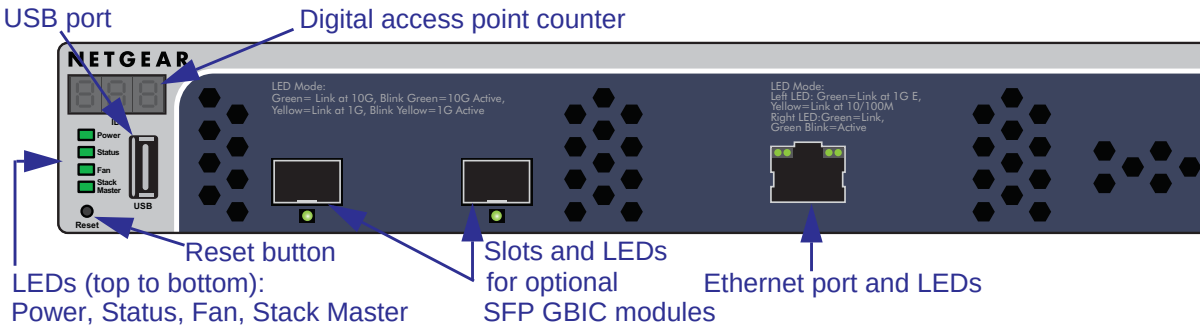


Figure 2. Front panel close-up

From left to right, the wireless controller's front panel shows the following counter, LEDs, button, ports, and slots:

- **Digital counter**. Displays the number of connected access points that are in a healthy state.
- From top to bottom:
  - **Power LED**
  - **Status LED**
  - **Fan LED**
  - **Stack Master LED**

  These LEDs are described in *Table 1* on page 12.
- **Reset button**. Using a sharp object, press and hold this button for about 10 seconds until the Status LED flashes and the wireless controller returns to factory default settings. If you reset the wireless controller, all configuration settings are lost and the default password is restored.
- **USB port**. Allows for external storage for floor heat maps, which will be supported in a future release.
- **SFP slots**. Two SFP slots for optional 10GE SFP+ or 1G SFP gigabit interface converters (GBICs), each slot with an LED.
- **Ethernet port**. One 10/100/1000 Mbps LAN Ethernet port with an RJ-45 connector, left LED, and right LED. The Ethernet port provides switched N-way, automatic speed negotiating, auto MDI/MDIX technology.
- **Console port**. RS232 port for connecting to an optional console terminal. The port has a DB9 male connector. The default baud rate is 9600 K. The configuration is 8 bits, no parity, and 1 stop bit. The console port is for debugging under guidance of NETGEAR technical support only.

The function of each LED is described in the following table:

Table 1. LED functions

LED	Status	Description
Power LED	Green	The green Power LED should be lit when the wireless controller is on.
	Off	If the power LED is not lit when the wireless controller is on, check the connections and check to see if the power outlet is controlled by a wall switch that is turned off (see *Power LED Is Not Lit* on page 198).
Status LED	Yellow	The wireless controller is initializing. After approximately two minutes, when the wireless controller has completed its initialization, the Status LED turns green. If the Status LED remains yellow, the initialization has failed (see *Status LED Never Turns Off* on page 198).
	Green	The wireless controller has completed its initialization successfully. The Status LED should be steady green during normal operation.

Table 1. LED functions (continued)

LED	Status	Description
Status LED (continued)	Off	The wireless controller does not have power.
	Blinking yellow	Firmware is being upgraded.
Fan LED	Green	The fans are functioning correctly.
	Yellow	One or more fans are not functioning correctly.
Stack Master LED	Green	The wireless controller functions as the primary controller (master) in a stack. (Stacking will be supported in a future release.)
	Yellow	The wireless controller functions as a secondary controller (slave) in a stack. (Stacking will be supported in a future release.)
SFP slot LEDs	Green	The slot is operating at 10G.
	Blinking green	Data is being transmitted or received at 10G.
	Yellow	The slot is operating at 1G.
	Blinking yellow	Data is being transmitted or received at 1G.
Left Ethernet port LED	Off	The port has no physical link, that is, no Ethernet cable is plugged into the wireless controller (see *Ethernet Port LEDs Are Not Lit* on page 199).
	Green	The port has detected a link with a connected Ethernet device.
	Blinking green	Data is being transmitted or received by the port.
Right Ethernet port LED	Off	The port has no physical link, that is, no Ethernet cable is plugged into the wireless controller (see *Ethernet Port LEDs Are Not Lit* on page 199).
	Green	The port is operating at 1000 Mbps.
	Yellow	The port is operating at 100 Mbps or 10 Mbps.

Back Panel Features

The wireless controller comes with a single internal power supply but supports an optional second power supply for power redundancy. The power supplies are hot-swappable.

The following figure shows the back panel components of the wireless controller with a single power supply.

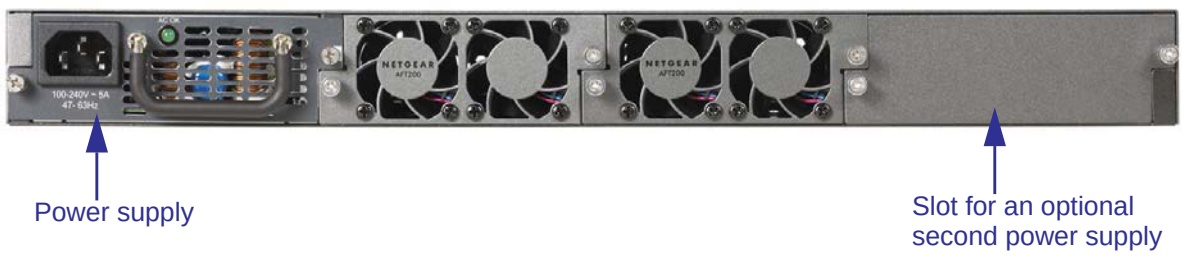


Figure 3. Back panel

From left to right, the wireless controller's back panel components are:

- **Power supply**. 100–240V, 5A, 47–63 Hz power supply, which includes the following external components:
  - **AC power socket**. Attach the power cord to this socket. (There is no separate on/off power switch.)
  - **Handle**. The handle allows for easy removal and insertion.
  - **LED**. The LED is lit green when the power supply functions correctly. If the LED is off, power is not supplied to the power supply, or there is a problem.
- **Fans**. Two double fans, each of which can be easily exchanged.

Bottom Panel with Product Label

The product label on the bottom of the wireless controller's enclosure displays the default IP address, default user name, and default password, as well as regulatory compliance, input power, and other information.

Figure 4. Product label

WC9500 Wireless Controller System Components

A WC9500 wireless controller *system* consists of one or more wireless controllers and a collection of access points that are organized into groups based on location or network access.

The wireless controller system can include a single wireless controller, a single wireless controller with a backup wireless controller for N:1 redundancy, or a group of up to three stacked wireless controllers, with or without a redundant wireless controller. Redundancy and stacking will be supported in a future release.

The WC9500 wireless controller system supports the following access point models:

- NETGEAR WNAP210v2 ProSAFE Wireless-N Access Point
- NETGEAR WNAP320 ProSAFE Wireless-N Access Point
- NETGEAR WNDAP350 ProSAFE Dual Band Wireless-N Access Point
- NETGEAR WNDAP360 ProSAFE Dual Band Wireless-N Access Point
- NETGEAR WNDAP380R ProSAFE Dual Band Wireless-N Access Point with RFID support

Future releases might support additional access point models.

NETGEAR ProSAFE Access Points

You can connect access points to the wireless controller either directly with an Ethernet cable through a router or switch, or remotely through an IP network. After you have used the automatic discovery process and added access points to the managed access point list on the wireless controller, the wireless controller converts the standard access points to dependent access points by pushing firmware to the access points. From then on, you can centrally manage and monitor the access points.

A WC9500 wireless controller system can support the following access points:

- **WNAP210v2 ProSAFE Wireless-N Access Point**
  - Supports 802.11b, 802.11g, and 802.11n network devices.
  - Supports Power over Ethernet (PoE) with a power consumption of up to 5.8W.
  - All WNAP210v2 firmware versions are supported.

  For product documentation and firmware, see *http://downloadcenter.netgear.com/en/product/WNAP210*.

  Note: *The WNAP210v1 (also referred to as just the WNAP210 without a version number) cannot function in a WC9500 wireless controller system, but the WNAP210v2 can.*

- **WNAP320 ProSAFE Wireless-N Access Point**
  - Supports 802.11b, 802.11g, and 802.11n network devices.
  - Supports Power over Ethernet (PoE) with a power consumption of up to 5.8W.
  - Accepts optional antennas.
  - Requires minimum firmware version 2.1.1 or a newer version.

  For product documentation and firmware, see *http://downloadcenter.netgear.com/en/product/WNAP320*.

- **WNDAP350 ProSAFE Dual Band Wireless-N Access Point**
  - Supports 802.11a, 802.11b, 802.11g, and 802.11n network devices.
  - Supports PoE with a power consumption of up to 10.75W.

- Concurrent operation in 2.4 GHz and 5 GHz radio band while in 802.11n mode.
- Accepts optional antennas.
- Requires minimum firmware version 2.1.7 or a newer version.

For product documentation and firmware, see *http://support.netgear.com/product/WNDAP350*.

- **WNDAP360 ProSAFE Dual Band Wireless-N Access Point**
  - Supports 802.11a, 802.11b, 802.11g, and 802.11n network devices.
  - Supports PoE with a power consumption of up to 10.51W.
  - Concurrent operation in 2.4 GHz and 5 GHz radio band while in 802.11n mode.
  - Accepts optional antennas.
  - Requires minimum firmware version 2.1.6 or a newer version.

  For product documentation and firmware, see *http://support.netgear.com/product/WNDAP360*.
- **WNDAP380R ProSAFE Dual Band Wireless-N Access Point with RFID support**
  - Supports 802.11a, 802.11b, 802.11g, and 802.11n network devices.
  - Supports PoE with a power consumption of up to 10.51W.
  - Concurrent operation in 2.4 GHz and 5 GHz radio band while in 802.11n mode.
  - Can integrate an RFID module for support of RFID devices and tags.
  - All WNDAP380R firmware versions are supported.

  For product documentation and firmware, see *http://support.netgear.com/product/WNDAP380R*.

What Can You Do with the WC9500 Wireless Controller?

These are some of the tasks that you can perform with a WC9500 wireless controller:

- **Organize the Network**
  - **Create access point profiles**. Organize access points in profiles to differentiate between SSIDs, client authentication, authentication settings, and wireless QoS settings.
  - **Create access point profile *groups***. Organize access point profiles in access point profile groups to differentiate between buildings, floors, businesses, business divisions, and so on. Easily assign access points to profile groups or change assignments.

  For more information, see *Chapter 5, Manage Security Profiles and Profile Groups*.

- **Discover Access Points in the Network and Provision IP Addresses and Firmware**
  - **Discover access points in the network**. The access points can be in factory default state or functioning in standalone mode, but after discovery by the wireless controller and addition to the managed access point list, the access points become dependent (managed) access points.
  - **Provision IP addresses to the access points**. Use the internal DHCP server to provision IP addresses to all or selected managed access points in the network.
  - **Upgrade access point firmware**. Update and synchronize new firmware versions to all managed access points in the network.

  For more information, see *Chapter 6, Discover and Manage Access Points*.
- **Centrally Manage Security in the Network**
  - **Manage secure access to the network and secure data transmission**. Manage client authentication, encryption, wireless client security separation, and MAC authentication in access point profiles.
  - **Manage authentication servers for the network**. Manage all internal and external authentication servers for the entire network or for access point profile groups.
  - **Manage MAC authentication**. Specify trusted and untrusted MAC addresses for the entire network.
  - **Manage rogue access points**. Manage rogue access points and their associated clients in the network.
  - **Manage guest access**. Manage guest access and captive portal access to the network.

  For more information, see *Chapter 7, Manage Rogue Access Points, Guest Network Access, and Users*.
- **Centrally Manage the Wireless Settings for the Network**
  - **Schedule the radios**. Schedule the entire network to go offline, or schedule access point profile groups to go offline.
  - **Manage wireless settings and channel allocation**. Manage the wireless settings such as wireless mode, data rate, and channel width for the entire network or for access point profile groups, and manage channel allocation for the entire network.
  - **Manage QoS settings**. Manage QoS queue settings for data, background, video, and voice traffic for access point profile groups.
  - **Configure RF management settings**. Configure WLAN healing and wireless coverage hole detection for the entire network or for access point profile groups.

  For more information, see *Chapter 8, Configure Wireless and QoS Settings*.
- **Monitor the Network and Its Components**
  - **Monitor the status of all wireless devices**. View the status of the wireless controllers, access points, clients, access point profiles, and the entire network, and view network usage statistics.
  - **Monitor network health**. See which access points are healthy and which ones are down or compromised.

For more information, see *Chapter 10, Monitor the Wireless Network and Its Components*.

Licenses

By default, the wireless controller comes with a trial license for five access points. You need to purchase and register licenses for the access points in your network. You can purchase a single 200–access point license or licenses in 10–, 50–, or 100–access point increments for support of up to 200 access points on a single wireless controller:

- **10–AP license**. WC10APL
- **50–AP license**. WC50APL
- **100–AP license**. WC100APL
- **200–AP license**. WC200APL

Licenses are tied to the serial number of the wireless controller.

For more information, see the datasheet that you can download from *http://support.netgear.com/product/WC9500*.

For information about how to register and manage your licenses, see *Register Your Licenses* on page 54 and *Manage Licenses* on page 165.

Maintenance and Support

NETGEAR offers technical support seven days a week, 24 hours a day. Information about support is available on the NETGEAR ProSupport website at *http://kb.netgear.com/app/answers/detail/a_id/212*.

System Planning and Deployment Scenarios

2

This chapter includes the following sections:

- *Basic and Advanced Setting Concepts*
- *Profile Group Concepts*
- *System Planning*
- *High-Level Configuration Examples*
- *Management VLAN and Data VLAN Strategies*
- *High-Level Deployment Scenarios*

Basic and Advanced Setting Concepts

You can deploy the wireless controller in a small wireless network with 10 or 20 access points or in a large wireless network with up to 600 access points. Small networks require a basic configuration, but large networks can become very complex and require you to configure the advanced features of the wireless controller.

Depending on your network configuration, use basic settings or advanced settings to manage your access points:

- **Basic settings for a typical network**. The basic settings work with most common network configurations. For example, all access points on the WLAN are for the same organization or business and therefore adhere to the same policies and use a small number of service set identifiers (SSIDs, or network names).
- **Advanced settings for access point profile groups**. If you have a large wireless network, or if separate networks share a single WLAN, use the advanced settings to set up multiple access point profile groups with multiple security profiles (SSIDs with associated security settings). For example, a shopping mall might need several access point profile groups if several businesses share a WLAN but each business has its own network. Larger networks could require multiple access point profile groups to allow different policies per building or department. The access points could have different security profiles per building and department, for example, one for guests, one for management, and one for sales.

Note: Access point profile groups are also referred to as just profile groups.
Profiles, security profiles, and SSIDs (that is, SSIDs with associated security settings) are terms that are interchangeable.

To accommodate all types of networks, almost all configuration menus of the web management interface are divided into basic and advanced submenus. The following figure shows an example of the Configuration > Security > Basic submenu on the left and the Configuration > Security > Advanced submenu on the right:

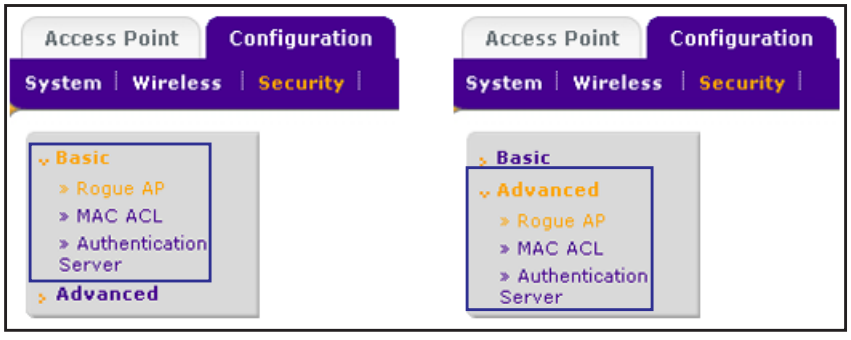


Figure 5. Basic and advanced submenus

Before you start the configuration of your wireless controller, decide whether you can use a basic configuration (that is, follow the Basic submenus) or need to use an advanced configuration (that is, follow the Advanced submenus). Once you have made your choice, configuring the wireless controller should be fairly easy if you consistently follow either the Basic submenus or the Advanced submenus.

Profile Group Concepts

Each access point can support up to eight security profiles (16 for dual-band access points), each with its own SSID, security settings, MAC ACL, rate-limiting settings, WMM, and so on.

The wireless controller follows the same architecture. A profile group on the wireless controller includes all the features that you can configure for an individual access point: up to eight profiles (16 for dual-band access points), each of which has its own SSID, security, MAC ACL, rate-limiting settings, WMM settings, and so on.

Basic Profile

The basic profile includes all the settings that are required to configure a fully functional access point with up to eight security profiles (16 for dual-band access points).

After you have used the automatic discovery process and added access points to the managed AP list on the wireless controller, the access points are assigned by default to the basic profile group.

If your network requires the wireless controller to manage multiple access points with different configurations, use the advanced profile.

Advanced Profile

The advanced profile lets you configure up to eight access point profile groups. Each group includes all the settings that are required to configure a fully functional access point with up to eight security profiles (16 for dual-band access points).

For example, if there are four buildings, each with a different wireless network, you simply create four profile groups. You then assign all access points in one building to one profile group, all access points in another building to a second profile group, and so on.

For each profile group, you can create an individual radio on/off schedule, RF management settings, MAC ACL authentication, and an authentication server. For each radio in a profile group (2.4 GHz radio and 5 GHz radio), you can create individual wireless settings, WMM, and rate-limit settings.

The following figure shows the advanced profile group architecture. The structure that is shown under Group-1 is implemented in all profile groups (that is, Group-2 through Group-8):

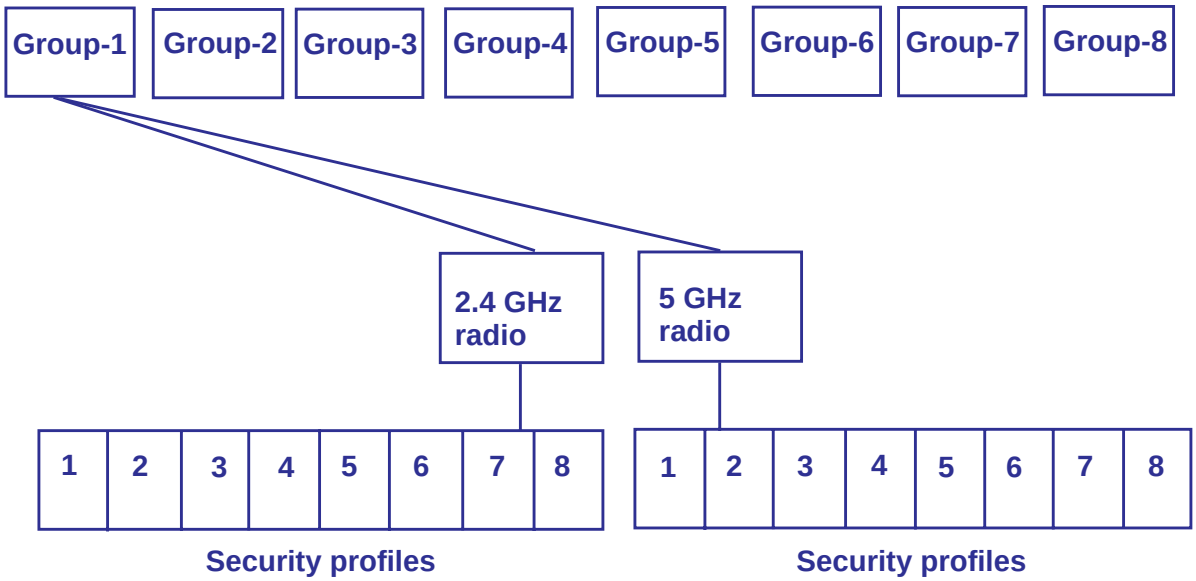


Figure 6. Advanced profile group architecture

The following figure shows an example of three access point profile groups, in which the first profile group (Group-1) has five security profiles. For each profile in this profile group, the profile name, radio mode, and authentication setting are shown. (Group-1 is the default group in the advanced profile group configuration; you need to create the other profiles groups.)

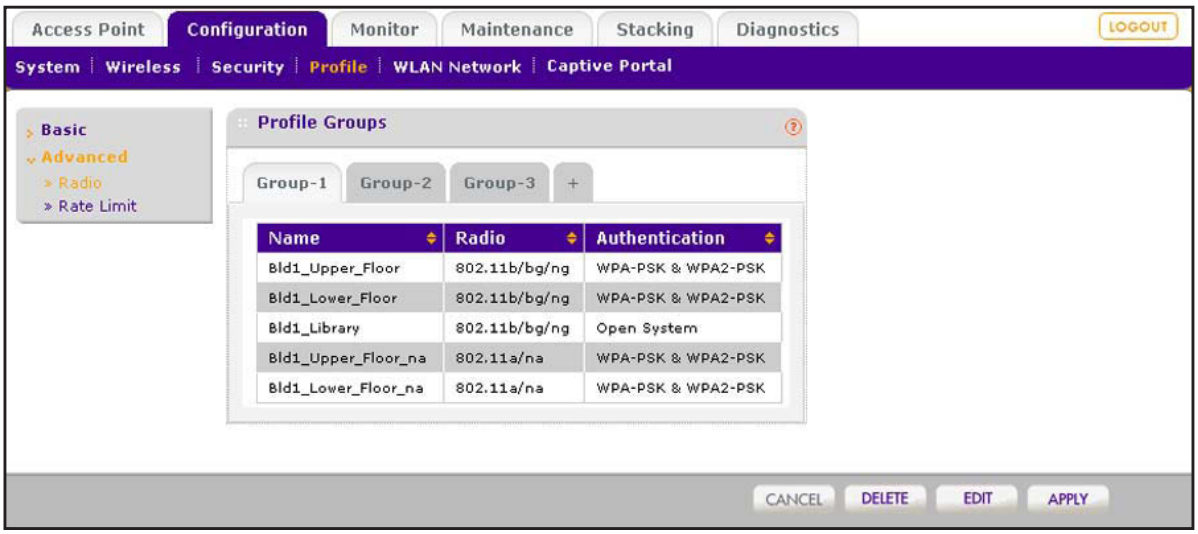


Figure 7. Example of profile groups with security profiles

System Planning

This section includes the following subsections:

- *Preinstallation Planning*
- *Before You Configure a Wireless Controller*

Preinstallation Planning

Before you install any wireless controllers, determine the following:

- Number of access points required to provide seamless coverage
- Number of licenses required to cover all access points that need to be managed
- Number of wireless controllers required
- 802.11 frequency band and the channels that are optimal for WiFi usage

NETGEAR recommends that you perform a site survey:

- Run a spectrum analysis of channels of the site to determine the current RF behavior and detect both 802.11 and non-802.11 noise.
- Run an access point-to-client connectivity test to determine the maximum throughput achievable on the client.
- Identify potential RF obstructions and interference sources.
- Determine areas where denser coverage might be required because of heavier usage.

Before You Configure a Wireless Controller

These sections assume that you have deployed at least one wireless controller in your network and are ready to configure the wireless controller. For information about how to deploy the wireless controller in your network, see the *ProSAFE Wireless Controller WC9500 Installation Guide* that you can download from *http://support.netgear.com/product/WC9500*.

For many configurations, you can use the default wireless settings. The IP address, VLAN, DHCP server, client authentication, and data encryption settings are specific to your environment. Following are short sections that describe these settings (except for IP address settings, which are self-explanatory). For information about how to configure these settings, see the relevant sections.

Management VLAN

The management VLAN is the dedicated VLAN for access to the wireless controller. All traffic that is directed to the wireless controller, including HTTP, HTTPS, SNMP, and SSH traffic, is carried over the management VLAN.

If the management VLAN is also configured as a tagged VLAN (the most common configuration), the packets to and from the wireless controller carry the 802.1Q VLAN header with the assigned VLAN number. If the management VLAN is marked as untagged, the

packets that are sent from the wireless controller do not carry the 802.1Q header, and all untagged packets that are sent to the wireless controller are treated as management VLAN traffic.

Note: Use a tagged VLAN or change the tagged VLAN ID only if the hubs and switches on your LAN support 802.1Q. If they do not, and you have not configured a tagged VLAN with the same VLAN ID on the hubs and switches in your network, IP connectivity might be lost.

The wireless controller needs to have IP connectivity with the access points through the management VLAN. If the wireless controller and the access points are on different management VLANs, external VLAN routing needs to allow IP connectivity between the wireless controller and the access points.

For information about how to configure management VLANs, see *IP and VLAN Settings* on page 49.

Client VLANs

Each authenticated wireless user is placed into a VLAN that determines the user's DHCP server, IP address, and Layer 2 connection. Although you could place all authenticated wireless users into the single VLAN that is specified in the basic security profile, the wireless controller allows you to group wireless users into separate VLANs based on the wireless SSID to differentiate access to network resources. For example, you might place authorized employee users into one VLAN, and itinerant users, such as contractors or guests, into a separate VLAN. To use different VLANs, you need to create different security profiles.

For information about how to configure regular VLANs, see *IP and VLAN Settings* on page 49.

DHCP Server

The wireless controller can function as a DHCP server and assign IP addresses to both wireless and wired devices that are connected to it. You can add up to 64 DHCP server pools, each assigned to a different VLAN.

Client Authentication and Data Encryption

A user needs to authenticate to the WLAN to be able to access WLAN resources. The wireless controller supports several types of security methods, including those that require an external RADIUS or LDAP authentication server.

The encryption option that you can select depends upon the authentication method that you have selected. The following table lists the authentication methods available, with their corresponding encryption options:

Table 2. Authentication and encryption options

Authentication Method	Encryption Option	Authentication Server
Open System	64-bit, 128-bit, or 152-bit WEP	None
Shared Key	64-bit, 128-bit, or 152-bit WEP	None
WPA-PSK	TKIP or TKIP+AES	None
WPA2-PSK	AES or TKIP+AES	None
WPA-PSK and WPA2-PSK	TKIP+AES	None
WPA	TKIP or TKIP+AES	One of the following authentication servers: • External RADIUS server • Internal authentication server • External LDAP server
WPA2	AES or TKIP+AES	One of the following authentication servers: • External RADIUS server • Internal authentication server • External LDAP server
WPA and WPA2	TKIP+AES	One of the following authentication servers: • External RADIUS server • Internal authentication server • External LDAP server

For information about how to configure client authentication, data encryption, and authentication servers, see *Chapter 5, Manage Security Profiles and Profile Groups*.

High-Level Configuration Examples

This section includes the following subsections:

- *Single Controller Configuration with Basic Profile Group*
- *Single Controller Configuration with Advanced Profile Groups*

Single Controller Configuration with Basic Profile Group

A basic configuration consists of a single wireless controller that controls a collection of access points that are organized into the basic default group.

➢ **To set up a single wireless controller system with a basic profile group:**

Step	Configuration	Web Management Interface Path
1.	Configure the system and network settings of the wireless controller:	
	1. Configure the country code of operation.	**Configuration > System > General**
	2. Configure the time settings.	**Configuration > System > Time**
	3. Configure the IP address of the wireless controller.	**Configuration > System > IP/VLAN**
	4. Verify that VLAN 1 is set as the management VLAN and is marked as untagged. By default, VLAN 1 an untagged management VLAN.	
	5. If no network DHCP server is accessible to the access points, configure the wireless controller's DHCP server.	**Configuration > System > DHCP Server**
2.	Configure up to eight profiles, and for each profile, do at least the following:	
	1. Configure an SSID for wireless access.	**Configuration > Profile > Basic**
	2. Configure the network authentication and data encryption.	
	3. Assign the VLAN.	
	4. If necessary for the selected network authentication option, configure the authentication server.	**Configuration > Security > Basic > Authentication Server**
3.	Run the Discovery Wizard and add the access points to the managed access point list.	**Access Point > Discovery Wizard**

Single Controller Configuration with Advanced Profile Groups

A more complex configuration consists of a single wireless controller that controls a collection of access points that are organized in access point profile groups and might use several profiles in each access point profile group.

➢ **To set up a single wireless controller system with advanced profile groups:**

Step	Configuration	Web Management Interface Path
1.	Configure the system and network settings of the wireless controller:	
	1. Configure the country code of operation.	**Configuration > System > General**
	2. Configure the time settings.	**Configuration > System > Time**
	3. Configure the IP address of the wireless controller.	**Configuration > System > IP/VLAN**
	4. Verify that VLAN 1 is set as the management VLAN and is marked as untagged. By default, VLAN 1 an untagged management VLAN.	
	5. If no network DHCP server is accessible to the access points, configure the wireless controller's DHCP server.	**Configuration > System > DHCP Server**
2.	Configure up to eight access point profile *groups*, and for each access point profile in a group, do at least the following:	
	1. Configure an SSID for wireless access.	**Configuration > Profile > Advanced**
	2. Configure the network authentication and data encryption.	
	3. Assign the VLAN.	
	4. If necessary for the selected network authentication option, configure the authentication server.	**Configuration > Security > Advanced > Authentication Server**
3.	Run the Discovery Wizard and add the access points to the managed access point list.	**Access Point > Discovery Wizard**
4.	Assign the access points to the access point profile *groups* (also referred to as WLAN groups).	**Configuration > WLAN Network**

Management VLAN and Data VLAN Strategies

If your network includes 10 or more access points, NETGEAR recommends that you set up at least two VLAN groups: a management VLAN group and a data VLAN group. If your network is large, you should create a number of data VLAN groups. Setting up data VLANs for clients allows you to:

- Segregate traffic by user category
- Create different policies such as access policies that are based on user category

The following illustration shows a simplified view of how you can use VLANs to segregate traffic by user category:

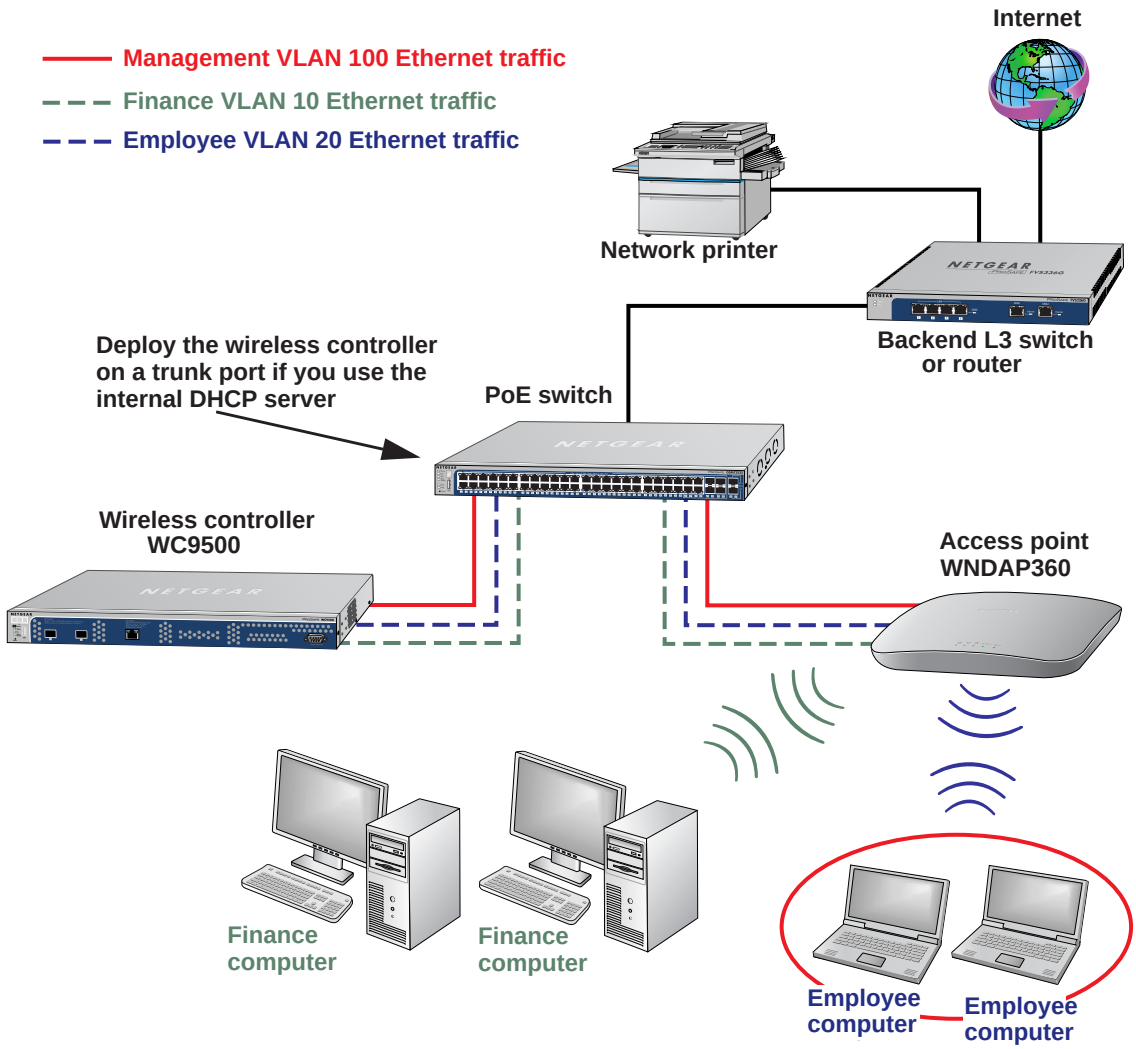


Figure 8. Example: Use VLANs to segregate traffic by user categories

The wireless controller uses the management VLAN to continually exchange packets with the access points. For large networks, if all traffic uses a single VLAN, the client traffic could potentially flood the network. If this happens, and the wireless controller is not able to exchange packets with the access points, it can cause network performance to slow down, and the access points can lose their connectivity with the wireless controller.

If you use the internal DHCP server of the wireless controller, you should deploy the wireless controller on a trunk port on your switch. The trunk port should have access to all VLANs. Use a high-speed port on your switch as the trunk port to accommodate the traffic load of the trunk. If you use an external DHCP server, you do not need to deploy the wireless controller on a trunk port on your switch.

High-Level Deployment Scenarios

This section provides three deployment scenarios to illustrate how the wireless controller can function in various network configurations:

- *Scenario Example 1: Network with Single VLAN*
- *Scenario Example 2: Advanced Network with VLANs and SSIDs*
- *Scenario Example 3: Advanced Network*

Scenario Example 1: Network with Single VLAN

The following sample scenario consists of a simple network with a wireless controller, PoE switch, Layer 3 switch or router, and access points:

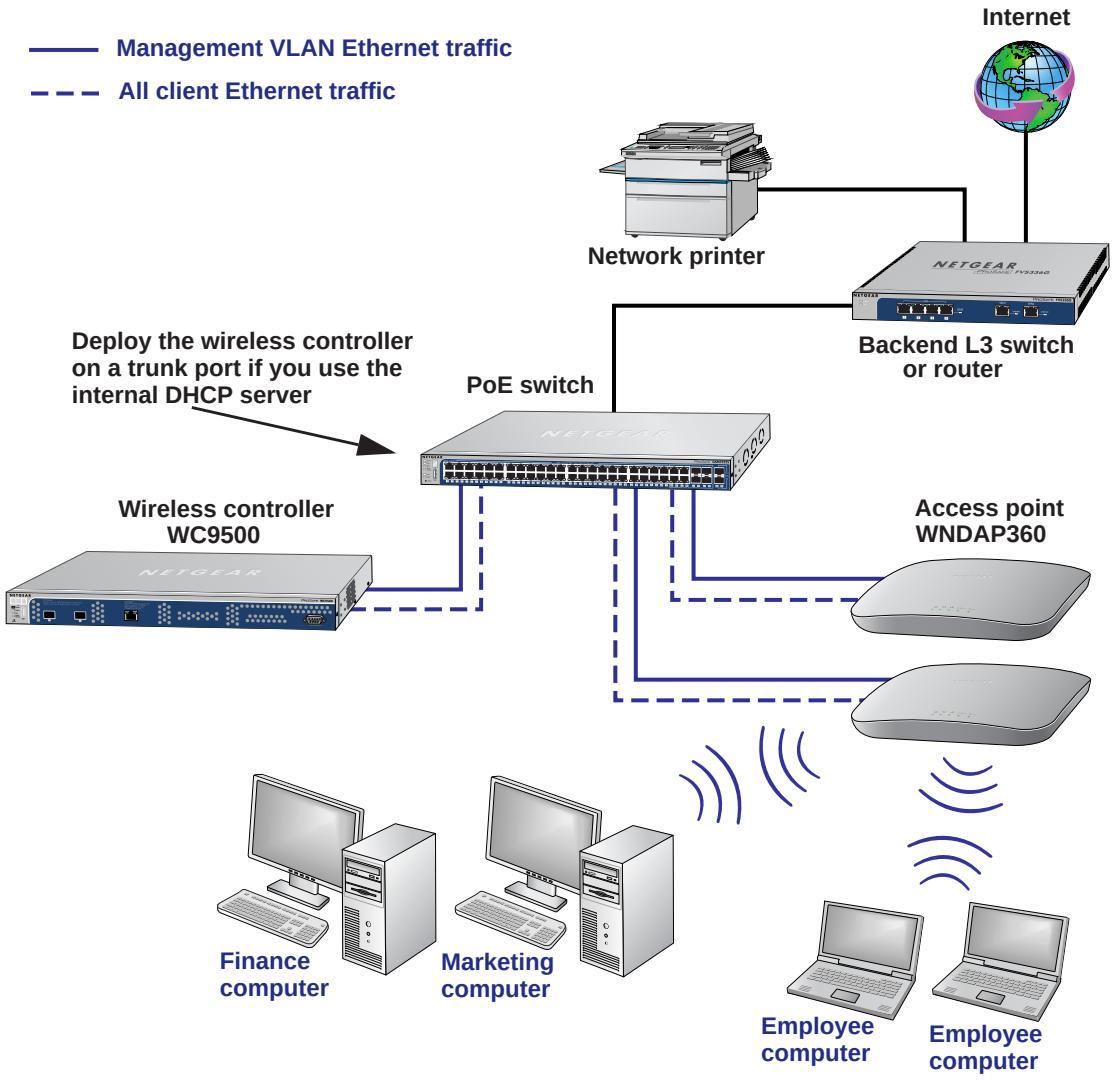


Figure 9. Example: Basic network with a single VLAN

The access points and wireless controller are connected in the same subnet and use the same IP address range that is assigned for that subnet. There are no routers between the access points and the wireless controller. The access points are connected to a PoE switch, which, in turn, is connected to the wireless controller. The uplink of the PoE switch connects to a Layer 3 switch or router that provides Internet access.

➢ **To provision the wireless controller:**

Step	Configuration	Web Management Interface Path
1.	Configure the system and network settings of the wireless controller:	
	1. Configure the country code of operation.	**Configuration > System > General**
	2. Configure the time settings.	**Configuration > System > Time**
	3. Configure the IP address of the wireless controller.	**Configuration > System > IP/VLAN**
	4. Verify that VLAN 1 is set as the management VLAN and is marked as untagged. By default, VLAN 1 an untagged management VLAN.	
	5. If no network DHCP server is accessible to the access points, configure the wireless controller's DHCP server.	**Configuration > System > DHCP Server**
2.	Configure up to eight profiles, and for each profile, do at least the following:	
	1. Configure an SSID for wireless access.	**Configuration > Profile > Basic**
	2. Configure the network authentication and data encryption.	
	3. Assign the VLAN.	
	4. If necessary for the selected network authentication option, configure the authentication server.	**Configuration > Security > Basic > Authentication Server**
3.	Use any port of the wireless controller to connect the wireless PoE switch.	
4.	Deploy the access points and connect them to the same wireless PoE switch.	

Step	Configuration	Web Management Interface Path
5.	When the access points are operating, open the Discovery Wizard to do the following:	Access Point > Discovery Wizard
	1. Specify the state of the access points by selecting the **Out of Factory and L2 Subnet APs** radio button or the **Installed and working in Standalone Mode** radio button.	
	2. Run the Discovery Wizard.	
	3. Select and add the access points that you want to be managed by the wireless controller to the managed list. **Note:** By default, all access points are added to the basic group and all settings from the basic group (profile definition, client authentication, authentication settings, and wireless QoS) are applied to the access points.	

Scenario Example 2: Advanced Network with VLANs and SSIDs

The following sample scenario consists of an advanced network with a wireless controller, PoE switch, Layer 3 switch or router, access points, and several VLANs and SSIDs. These are the VLANs in the wireless controller system:

- VLAN 1, the default untagged VLAN to access the wireless controller
- VLAN 10, a tagged client VLAN
- VLAN 20, another tagged client VLAN
- VLAN 100, a tagged management VLAN

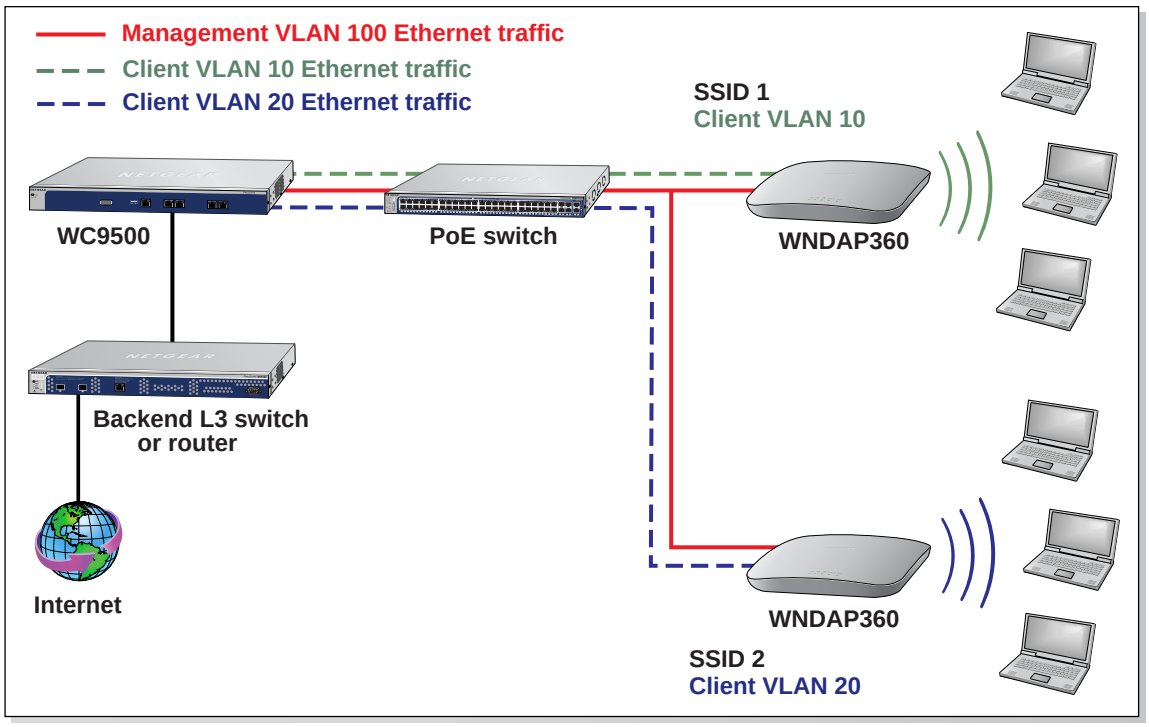


Figure 10. Example: Advanced network with VLANs and SSIDs

The access points and wireless controller are connected in the same subnet and same VLAN and use the same IP address range that is assigned for that subnet. There are no routers between the access points and the wireless controller. The access points are connected to a PoE switch, which, in turn, is connected to the wireless controller. The uplink of the PoE switch connects to a Layer 3 switch or router that provides Internet access.

This network configuration has the following prerequisites:

- VLANs 10, 20, and 100 are tagged VLANs and are configured on both the wireless controller and the PoE switch.
- The wireless controller is connected to the PoE switch through default VLAN 1. You manage the wireless controller from a computer over VLAN 1 through the PoE switch.
- The DHCP server on the wireless controller is configured in management VLAN 100 to enable the access points to receive an IP address through VLAN 100.
- The PoE switch port to which the wireless controller is connected is configured as a tagged port to allow tagged traffic from VLAN 100.

To provision the wireless controller:

Step	Configuration	Web management interface path
1.	Configure the basic system settings:	
	1. Configure the country code of operation.	**Configuration > System > General**
	2. Configure the time settings.	**Configuration > System > Time**
	3. Configure the IP address of wireless controller.	**Configuration > System > IP/VLAN**
	4. For initial discovery and configuration of the access points, temporarily configure management VLAN 100 as an untagged management VLAN on the wireless controller.	
	5. Clear the **Untagged Vlan** check box. Default VLAN 1 changes to a tagged VLAN.	
2.	For initial discovery and configuration of the access points, temporarily configure management VLAN 100 as an untagged management on the PoE switch.	
3.	Configure either the network's DHCP server or the wireless controller's DHCP server to use VLAN 100. If you use the wireless controller's DHCP server:	
	1. Configure the IP address range for VLAN 100.	**Configuration > System > DHCP Server**
	2. Configure the other DHCP server fields, including the gateway and DNS servers.	
4.	Configure the following profiles, and configure network authentication and data encryption for these profiles:	
	1. A profile with SSID 1 and VLAN 10.	**Configuration > Profile > Basic**
	2. A profile with SSID 2 and VLAN 20.	
	3. If necessary for the selected network authentication options, configure one or more authentication servers.	**Configuration > Security > Basic > Authentication Server**
5.	Connect the wireless controller to the PoE switch.	
6.	Before you connect the access points to the PoE switch, verify that the switch ports to which you intend to connect the access points are configured as access ports in management VLAN 100.	
7.	Deploy the access points and connect them to the designated PoE switch ports.	

Step	Configuration	Web management interface path
8.	When the access points are operating, open the Discovery Wizard to do the following:	**Access Point > Discovery Wizard**
	1. Specify the state of the access points by selecting the **Out of Factory and L2 Subnet APs** radio button.	
	2. Run the Discovery Wizard.	
	3. Select and add the access points that you want to be managed by the wireless controller to the managed list. **Note:** By adding the access points to managed list, you enable them to receive an IP address from the DHCP server over management VLAN 100.	
9.	For each access point on the managed list, clear the **Untagged Vlan** check box and configure VLAN 100 as the management VLAN. Doing so causes the access points to lose connectivity with the wireless controller.	
10.	Restore connectivity between the access points and the wireless controller by changing the PoE switch ports to which the access points are connected to tagged ports. During the discovery process, these switch ports were access ports in management VLAN 100.	

Scenario Example 3: Advanced Network

The following sample scenario consists of an advanced network with one wireless controller, one core switch, two PoE switches in different buildings, access points, and several VLANs and SSIDs.

These are the components in the wireless controller system:

- One wireless controller
- 50 access points (managed by the wireless controller through management VLAN 1)
- Four VLANs: VLAN 10, VLAN 20, VLAN 30, and VLAN 40
- Three SSIDs: SSID 1, SSID 2, and SSID 3

In this scenario, the VLANs and SSIDs are used to accommodate traffic for different user groups in a school that is spread out over two buildings.

- Building 1:
  - SSID 1 in VLAN 10 for staff traffic
  - SSID 2 in VLAN 20 for middle school students
  - SSID 3 in VLAN 30 for guests

- Building 2:
  - SSID 1 in VLAN 10 for staff traffic
  - SSID 2 in VLAN 40 for high school students
  - SSID 3 in VLAN 30 for guests

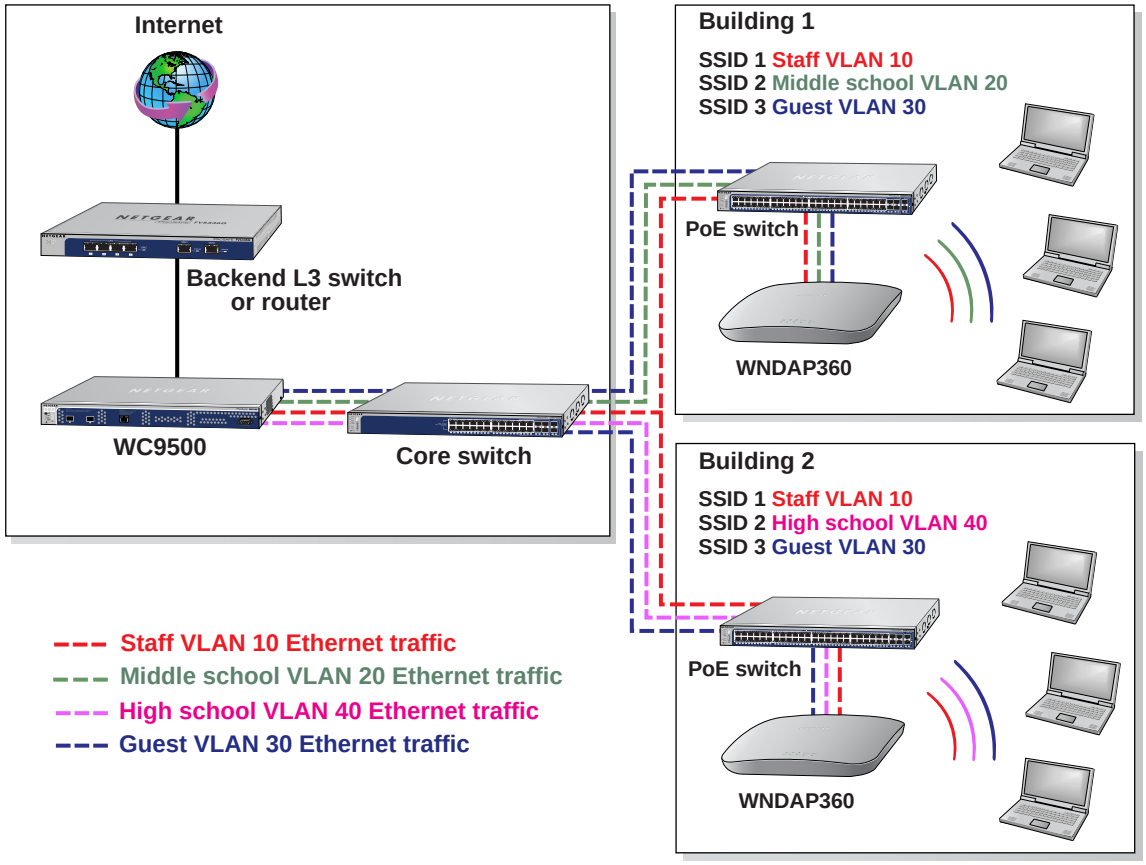


Figure 11. Example: Advanced network

The access points and wireless controllers are connected in the same subnet and same VLAN and use the same IP address range that is assigned for that subnet. The core switch is located between the wireless controllers and the PoE switches, to which the access points are connected. The core switch provides Internet access.

This network configuration has the following prerequisites:

- VLAN 1 is configured on the wireless controllers, core switch, and PoE switches. This VLAN is untagged.
- VLANs 10, 20, and 30 are configured on the wireless controllers, core switch, and the PoE switch in Building 1. These VLANs are tagged.
- VLANs 1, 10, 20, 30, and 40 are configured on the wireless controllers, core switch, and PoE switches. Except for VLAN 1, these VLANs are tagged.

➢ To provision the wireless controller:

Step	Configuration	Web management interface path
1.	Configure the basic system settings:	
	1. Configure the country code of operation.	**Configuration > System > General**
	2. Configure the time settings.	**Configuration > System > Time**
	3. Configure the IP address of wireless controller.	**Configuration > System > IP/VLAN**
	4. Verify that VLAN 1 is set as the management VLAN and is marked as untagged. By default, VLAN 1 an untagged management VLAN.	
2.	Configure the following profiles, and configure network authentication and data encryption for these profiles:	
	1. A profile with SSID 1 and VLAN 10.	**Configuration > Profile > Basic**
	2. A profile with SSID 2 and VLAN 20.	
	3. A profile with SSID 2 and VLAN 30.	
	4. A profile with SSID 3 and VLAN 40.	
	5. If necessary for the selected network authentication options, configure one or more authentication servers.	**Configuration > Security > Basic > Authentication Server**
3.	Configure the following profile groups:	
	1. A profile group with the name Building 1, to which you add the following profiles: - The profile with SSID 1 and VLAN 10 - The profile with SSID 2 and VLAN 20 - The profile with SSID 2 and VLAN 30	**Configuration > Profile > Advanced**
	2. A profile group with the name Building 2, to which you add the following profiles: - The profile with SSID 1 and VLAN 10 - The profile with SSID 2 and VLAN 30 - The profile with SSID 3 and VLAN 40	
4.	Deploy the access points and connect them to PoE switches.	

Step	Configuration	Web management interface path
5.	When the access points are operating, open the Discovery Wizard to do the following:	**Access Point > Discovery Wizard**
	1. Specify the state of the access points by selecting the **Out of Factory and L2 Subnet APs** radio button.	
	2. Run the Discovery Wizard.	
	3. Select and add the access points that you want to be managed by the wireless controller to the managed list. **Note:** By default, all access points are added to the basic group.	
6.	Assign the access points to the access point profile *groups* (also referred to as WLAN groups) Building 1 and Building 2.	**Configuration > WLAN Network**

Installation and Configuration Overview

3

This chapter includes the following sections:

- *Initial Set up and Log in*
- *Web Management Interface Layout*
- *Roadmap for Initial Configuration*
- *Roadmap for Configuring Management of Your Wireless Network*
- *Choose a Location for the Wireless Controller*
- *Deploy the Wireless Controller*

Initial Set up and Log in

To set up and log in to the wireless controller, follow the steps in this section. You can also access the *ProSAFE Wireless Controller WC9500 Installation Guide* that you can download from *http://support.netgear.com/product/WC9500*.

Note: To log in to the wireless controller, you need to use a web browser such as Microsoft Internet Explorer 8 or later or Mozilla Firefox 18 or later, or Google Chrome 24 or later with JavaScript, cookies, and SSL enabled.

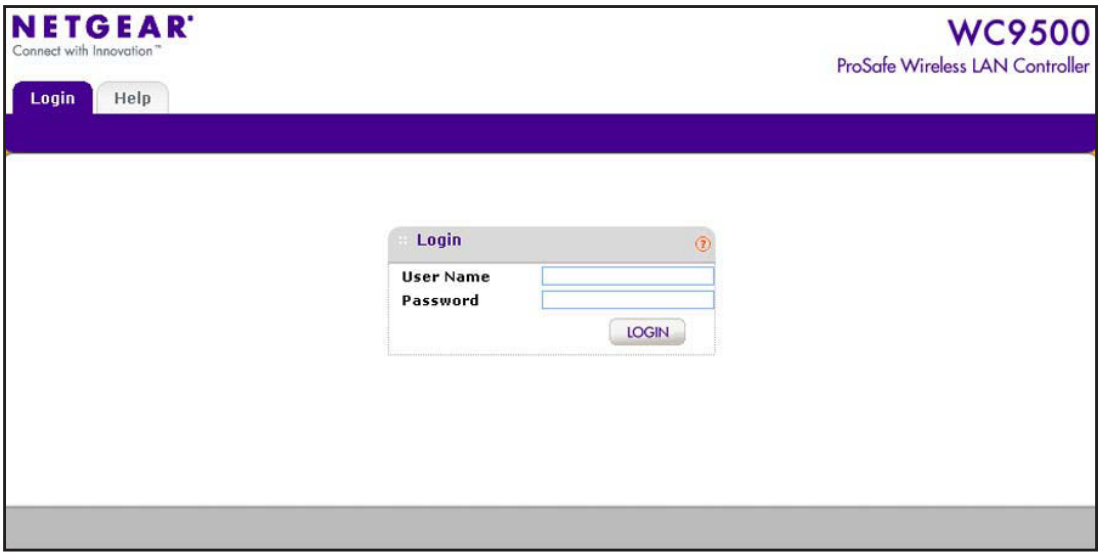
➢ **To set up and log in to the wireless controller:**

1. Connect the wireless controller to your computer:
   a. Configure a computer with a static IP address of 192.168.0.210 and 255.255.255.0 as the subnet mask.
   b. Connect the wireless controller to the computer through the network or directly to the wireless controller's Ethernet port.
   c. Connect the power cord from the wireless controller to an AC power outlet.
   d. Verify that the following LEDs on the front panel are lit:

LED	Description
Power	The green Power LED is lit. If the Power LED is not lit, check the connections and check to see if the power outlet is controlled by a wall switch that is turned off.
Status	The Status LED is lit yellow while the wireless controller is initializing. After approximately two minutes, when the wireless controller has completed its initialization, the Status LED turns green.
Fan	The green Fan LED is lit, indicating that the fans are functioning correctly.
Ethernet	The right Ethernet port LED is lit green for a 1000 Mbps connection or yellow for a 100 Mbps or 10 Mbps connection. If it is not, make sure that the Ethernet cable is securely attached at both ends.

2. Log in to the wireless controller:
   a. Open your browser and type **http://192.168.0.250** in the browser's address field.

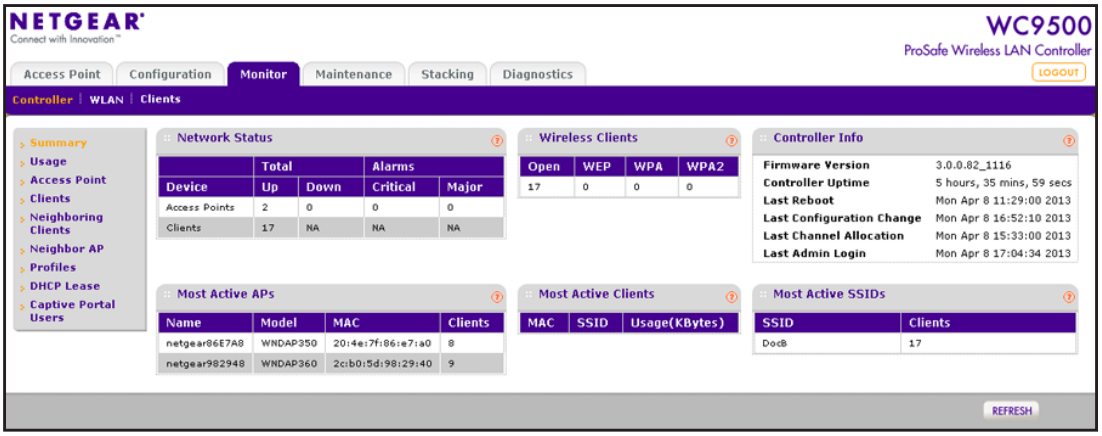
The wireless controller's login screen displays:



b. When prompted, enter **admin** for the user name and **password** for the password, both in lowercase letters.

c. Click **Login**.

The wireless controller's web management interface opens and displays the Summary screen (the path is Monitor > Controller > Summary), which shows the network status and related information:



For information about the network status and related information, see *View the Wireless Controller Summary Screen* on page 173.

For information about the layout and general characteristics of the web management interface, see the following section, *Web Management Interface Layout*.

Web Management Interface Layout

The following figure shows the menus at the top and the left of the wireless controller's web management interface (the screen's content has been removed for more clarity).

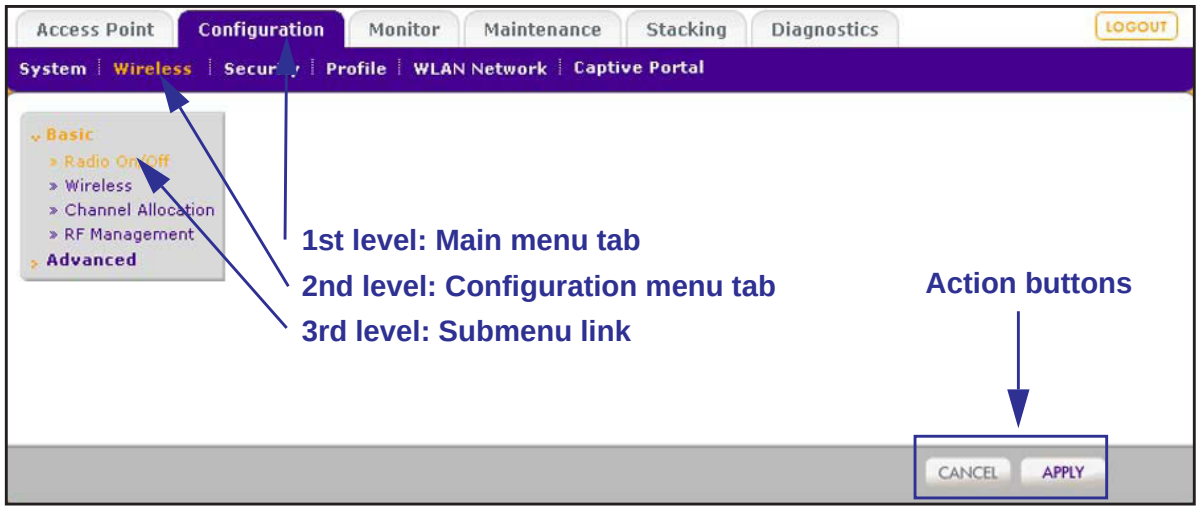


Figure 12. Web management interface components

A web management interface screen can include the following components:

- **1st level: Main menu tab**. The main menu tabs in the light gray bar across the top of the web management interface provide access to all configuration menu tabs of the wireless controller and remain constant. When you select a main menu tab, the letters are displayed in white against a blue background.
- **2nd level: Configuration menu tab**. The configuration menu tabs in the blue bar (immediately below the main menu bar) change according to the main menu tab that you select. When you select a configuration menu tab, the letters are displayed in orange against a blue background.
- **3rd level: Submenu link**. Each configuration menu tab has one or more submenu links that are listed on the left side of the screen in a gray box. When you select a submenu link, the text is displayed in orange against a gray background. On many screens, the submenus are divided into a Basic submenu and an Advanced submenu.
- **Action buttons**. Action buttons let you change the configuration or navigate through the web management interface. These are the most common action buttons:
  - **Apply**. Saves all configuration changes made on the current screen. Saved settings are retained when the wireless controller is powered off or rebooted, while unsaved configuration changes are lost.
  - **Cancel**. Resets options on the current screen to the last-applied or -saved settings.
  - **Add**. Adds an item to the screen. Typically, a pop-up screen opens that enables you to enter information in additional fields.
  - **Edit**. Allows you to edit the configuration of the selected item.

- **Delete** or **Remove**. Removes the selected item from the table or screen configuration.
- **Back**. Return to the previous screen.
- **Next**. Advance to the next screen.

Roadmap for Initial Configuration

After you have connected and logged in to the wireless controller, you need to perform the initial configuration. If you are not sure how you are going to deploy the wireless controller in your network, NETGEAR recommends that you read *Chapter 2, System Planning and Deployment Scenarios*.

This section is a roadmap for basic configuration only: It provides *high-level* configuration steps with references to the sections or chapters that provide detailed configuration steps.

➢ **To perform the initial configuration of the wireless controller:**

1. Select **Configuration > System > General**.

   The General Settings screen displays.

2. Enter a name for the wireless controller and select the country in which the wireless controller is used.
3. Click **Apply**.
4. Select **Configuration > System > Time**.

   The Time Setting screen displays.

5. Select the time zone in which the wireless controller is used. Optionally, configure the NTP settings.

   For more information, see *Manage the Time Settings* on page 48.

6. Click **Apply**.
7. Select **Configuration > System > IP/VLAN**.

   The IP Settings screen displays.

8. Enter the IP settings for your network and the VLANs that you want to assign to the wireless controller.

   Note: *A management VLAN is used for all SNMP and HTTP traffic to and from the wireless controller and managed access points.*

   Note: *Clear the Untagged VLAN check box only if the hubs and switches in your network support the VLAN (802.1Q) standard. Likewise, change the untagged VLAN value only if the hubs and switches in your network support the VLAN (802.1Q) standard.*

   For more information, see *IP and VLAN Settings* on page 49.

9. Click **Apply**.
10. (Optional) If no DHCP server is available in your network, configure the wireless controller's DHCP server.

    For more information, see *Manage the DHCP Server* on page 51.
11. Click **Apply**.

    The connection to the wireless controller is terminated because you have changed its IP address.
12. Reconfigure your computer with an IP address and subnet mask that is in the same IP subnet as the new IP address of the wireless controller.
13. Log back in to the wireless controller using its new IP address.

    Continue with the following section, *Roadmap for Configuring Management of Your Wireless Network*.

Roadmap for Configuring Management of Your Wireless Network

After you have performed the initial configuration and changed the IP address to an address that is specific to your network (see the previous section, *Roadmap for Initial Configuration*), you are ready to configure the wireless controller for management of your wireless network.

This section is a roadmap only: It provides *high-level* configuration steps with references to the sections or chapters that provide detailed configuration steps.

➢ **To configure the wireless controller for management of your wireless network:**

1. Register the licenses.

   For more information, see *Register Your Licenses* on page 54.
2. (Optional but recommended) Replace the default certificate with a custom certificate for certificate-based authentication of the internal authentication server.

   For more information, see *Manage Certificates* on page 57.
3. (Optional but recommended) Configure logs, alerts, and alarms.

   For more information, see *Configure Log, Syslog, Alarm Notification, and Email Settings* on page 58.
4. Configure security profiles:
   a. Configure the security profiles for the basic profile group or for advanced profile groups.

      For detailed configuration steps, see:

      - *Configure Security Profiles for the Basic Profile Group* on page 67
      - *Configure Security Profiles for Advanced Profile Groups* on page 71

   b. (Optional) Configure authentication servers.

For more information, see *Manage Authentication Servers and Authentication Server Groups* on page 85.

c. (Optional) Configure MAC authentication.

For more information, see *Manage MAC Authentication and MAC Authentication Groups* on page 81.

d. (Optional) Assign the authentication servers and MAC ACLs to the security profiles.

For more information, see:

- *Configure Security Profiles for the Basic Profile Group* on page 67
- *Configure Security Profiles for Advanced Profile Groups* on page 71

5. Configure the managed access point list:

a. Run the Discovery Wizard and add access points to the managed list.

For more information, see *Discover Access Points with the Discovery Wizard* on page 92.

b. (Optional) Configure access points that are on the managed list.

For more information, see *Manage the Managed AP List* on page 100.

c. (Optional) Assign access points to advanced profile groups:

For more information, see *Assign Access Points to Advanced Profile Groups* on page 104.

6. (Optional) Configure rogue access point detection.

For more information, see *Manage Rogue Access Points* on page 108.

7. (Optional) Configure a guest portal or captive portal.

For more information, see *Manage Guest Network Access* on page 111.

8. (Optional) Configure user accounts and portal accounts.

For more information, see *Manage Users, Accounts, and Passwords* on page 116.

9. (Optional) Configure wireless and QoS settings.

For more information, see *Chapter 8, Configure Wireless and QoS Settings*.

10. (Optional but recommended) Back up the configuration.

For more information, see *Back Up the Configuration File* on page 152.

Choose a Location for the Wireless Controller

The wireless controller is suitable for use in an office environment where it can be freestanding on its runner feet or mounted into a standard 19-inch equipment rack. Alternatively, you can rack-mount the wireless controller in a wiring closet or equipment room. A mounting kit, containing two mounting brackets and screws, is provided in the wireless controller package.

Consider the following when deciding where to position the wireless controller:

- The unit is accessible and cables can be connected easily.
- Cabling is away from sources of electrical noise. These include lift shafts, microwave ovens, and air-conditioning units.
- Water or moisture cannot enter the case of the unit.
- Airflow around the unit and through the vents in the side of the case is not restricted. Provide a minimum of 25 mm or one inch clearance.
- The air is as free of dust as possible.
- Temperature operating limits are not likely to be exceeded. Install the unit in a clean, air-conditioned environment. For information about the recommended operating temperatures for the wireless controller, see *Appendix A, Factory Default Settings and Technical Specifications*.

Deploy the Wireless Controller

After you have followed the steps in the *Roadmap for Initial Configuration* on page 42 and the *Roadmap for Configuring Management of Your Wireless Network* on page 43, you are ready to deploy the wireless controller in your network.

➢ **To deploy the wireless controller:**

1. Disconnect the wireless controller from the computer that you used for configuration.
2. (Optional) Reconfigure the computer back to its original TCP/IP settings.
3. Place the wireless controller where you intend to deploy it.
4. Connect an Ethernet cable from the wireless controller to a switch or router on your wired network.
5. Connect the power cord to the wireless controller and plug the power cord into a power outlet.

   The Power, Status, and Ethernet LEDs should light. If any of these do not light, see *Troubleshoot Basic Functioning* on page 198.

Configure the System and Network Settings and Register the Licenses

4

This chapter includes the following sections:

- *Configure General Settings*
- *Manage the Time Settings*
- *IP and VLAN Settings*
- *Manage the DHCP Server*
- *Register Your Licenses*
- *Manage Certificates*
- *Configure Log, Syslog, Alarm Notification, and Email Settings*

Configure General Settings

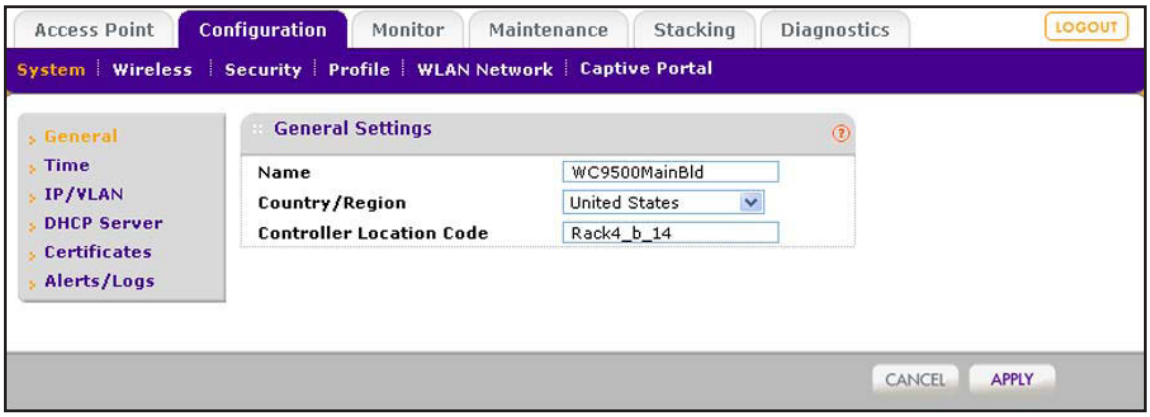
Note: You need to select the correct country or region of operation. It might not be legal to operate the access points in a country or region not shown here. If your location is not listed, check with your local government agency or check the NETGEAR website for more information about which channels to use.

The General Settings screen lets you configure the basic settings of your wireless controller.

➢ **To configure general settings:**

1. Select **Configuration > System > General**.

   The General Settings screen displays:



2. Configure the settings as described in the following table:

Setting	Description
Name	Enter a unique value as the wireless controller name. NETGEAR recommends changing the name as soon as possible after setting up. The name needs to contain only alphabetical characters, numbers, and hyphens, and needs to be 31 characters or less.
Country/Region	From the menu, select the region of operation for the wireless controller and the access points managed by the wireless controller. This setting is crucial for optimal performance of the wireless controller. The wireless controller uses the country code to determine the best wireless settings for your access points. In the United States, the country is preset and cannot be changed on the access points. If the country or region is not set up correctly, the wireless controller might not be able to access the access points.
Controller Location Code	(Optional) Enter a code to identify the physical location of the wireless controller. This is especially useful if you use more than one wireless controller.

3. Click **Apply**.

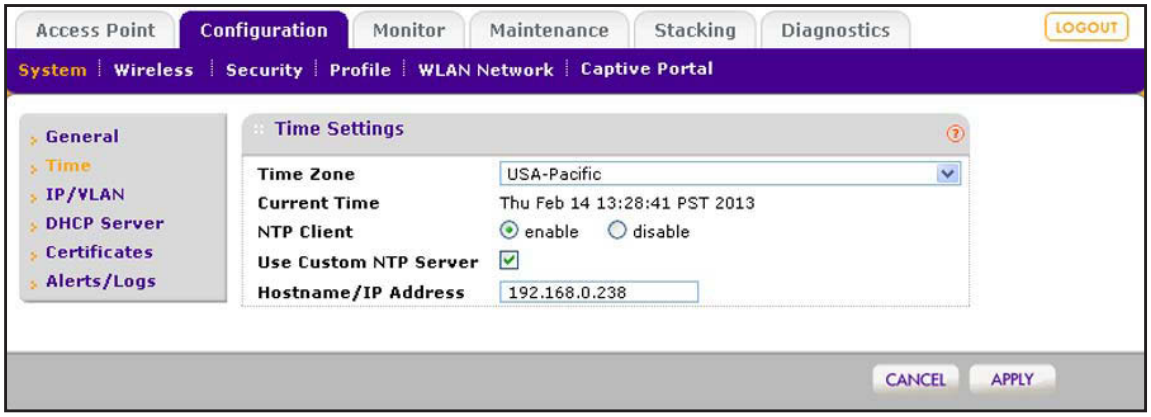
Manage the Time Settings

This screen lets you configure the time-related settings of your wireless controller and managed access points.

➢ **To configure time settings:**

1. Select **Configuration > System > Time**.

   The Time Settings screen displays:



2. Configure the settings as described in the following table:

Setting	Description
Time Zone	From the menu, select the local time zone for your country or region.
Current Time	This is a nonconfigurable field that displays the current time at your location.
NTP Client	Select the **Enable** radio button to use a Network Time Protocol (NTP) server to synchronize the clock of the wireless controller and managed access points. Select the **Disable** radio button if you do not want to use an NTP server.
Use Custom NTP Server	Select this check box if you want to use an alternate NTP server. By default, the NETGEAR NTP server is used.
Hostname/IP Address	Enter the host name or IP address of the NTP server, if you are using a custom NTP server.

3. Click **Apply**.

IP and VLAN Settings

The IP Settings screen lets you configure the management IP address and VLAN settings of the wireless controller.

Management VLAN Concepts

Management VLANs are used for all SNMP and HTTP traffic to and from the wireless controller and managed access points.

For large deployments, NETGEAR recommends that the wireless controller and access points are in separate VLANs to ensure uninterrupted connectivity between the wireless controller and the access points.

The wireless controller and access points share heartbeat messages to keep synchronized and share configurations and client key data to facilitate seamless roaming.

Untagged VLAN Concepts

When the Untagged VLAN check box is selected on the IP Settings screen, one VLAN can be configured as an untagged VLAN:

- When the wireless controller sends frames associated with the untagged VLAN to the LAN (Ethernet) interface, those frames do not carry an 802.1Q VLAN header.
- When the wireless controller receives untagged traffic from the LAN (Ethernet) interface, those frames are assigned to the untagged VLAN.

If the Untagged VLAN check box is cleared, the wireless controller tags all outgoing LAN (Ethernet) frames, and accepts only incoming frames that are tagged with known VLAN IDs.

Note: Clear the Untagged VLAN check box only if the hubs and switches on your LAN support the VLAN (802.1Q) standard. Likewise, change the untagged VLAN value only if the hubs and switches on your LAN support the VLAN (802.1Q) standard.

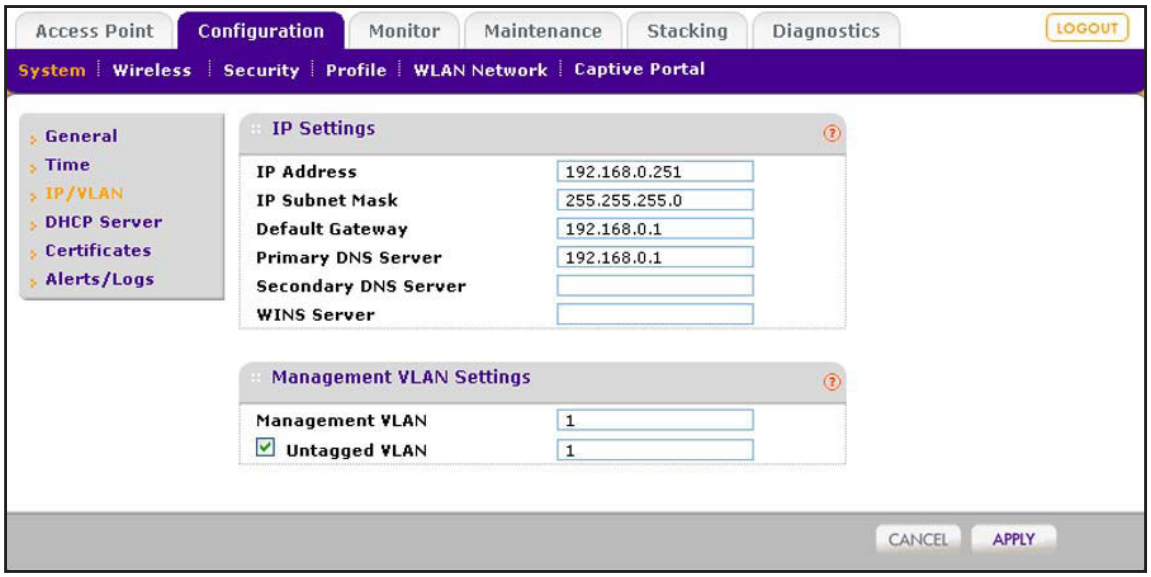
Changing either of these values results in a loss of IP connectivity if the hubs and switches on your network have not yet been configured with the corresponding VLANs.

Configure the IP and VLAN Settings

➢ **To configure IP/VLAN settings:**

1. Select **Configuration > System > IP/VLAN**.

The IP Settings screen displays:



2. Configure the settings as described in the following table:

Setting	Description
IP Settings section	
IP Address	Enter the IP address of the wireless controller. The default IP address is 192.168.0.250. To change it, enter an available IP address from the address range used on your LAN.
IP Subnet Mask	Enter the subnet mask value used on your LAN. The default value is 255.255.255.0.
Default Gateway	Enter the IP address of the gateway for your LAN.
Primary DNS Server	Enter the IP address of the primary Domain Name Server (DNS) that you want to use.
Secondary DNS Server	Enter the IP address of the secondary DNS that you want to use.
WINS Server	Enter the IP address of the Windows Internet Name Service (WINS) that you want to use.
Management VLAN Settings section	
Management VLAN	Enter the management VLAN. For information, see *Management VLAN Concepts* on page 49.
Untagged VLAN	Select this check box if the configured VLAN is untagged. For information, see *Untagged VLAN Concepts* on page 49.

3. Click **Apply**.

Manage the DHCP Server

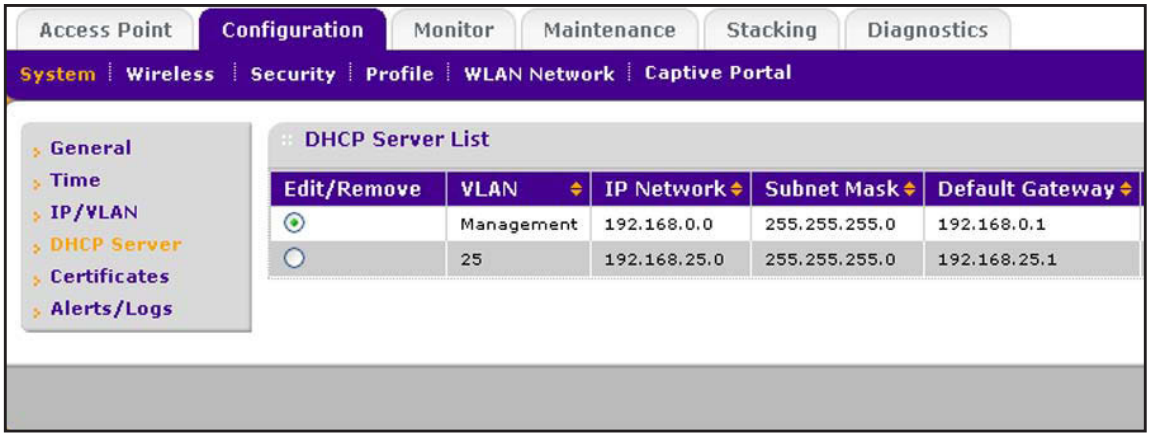
Note: Make sure that a DHCP server is available; otherwise, the Discovery Wizard does not function correctly. If you already have a DHCP server on your network, do not enable the DHCP server on the wireless controller.

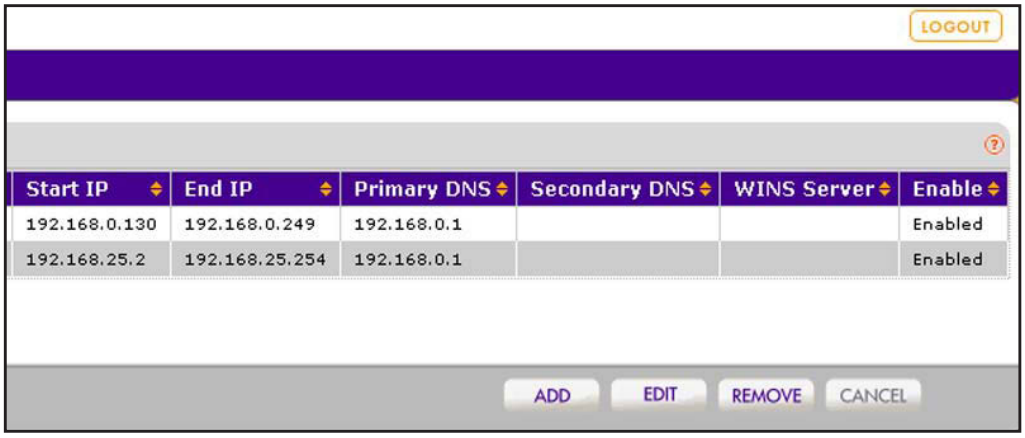
The wireless controller can function as a DHCP server. You can add multiple DHCP server pools for different VLANs. By default, there is no DHCP server pool. The DHCP Server List screen lets you add a DHCP server pool.

➢ **To add a DHCP server and configure its settings:**

1. Select **Configuration > System > DHCP Server**.

   The DHCP Server List screen displays. The following figure shows part of the DHCP Server List screen. Because this is a wide screen, it is shown in the following two figures:

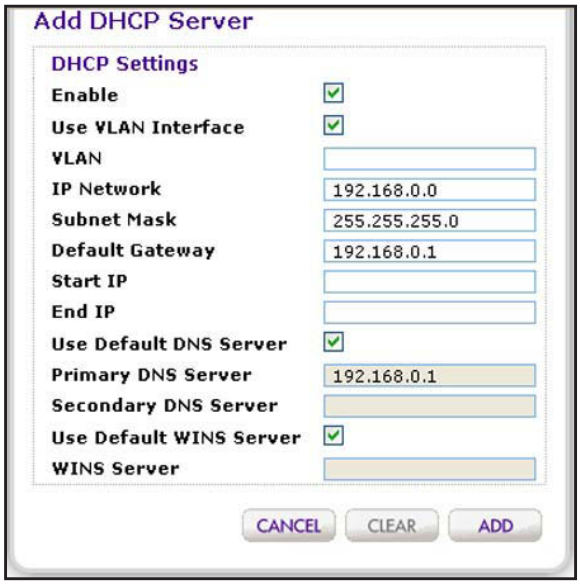




   The DHCP Server List shows the DHCP servers that are already configured on the wireless controller.

2. Click **Add**.

   The Add DHCP Server pop-up screen displays:



3. Configure the settings as described in the following table:

Setting	Description
Enabled	Select this check box to enable the DHCP server. When the check box is cleared, the DHCP server is disabled.
Use VLAN Interface	Select this check box to allow the DHCP server to function with multiple VLANs.
VLAN	Enter the DHCP server VLAN ID. The range is between 1 and 4094. The DHCP server services this VLAN.
IP Network	Enter the IP address for the wireless controller in the VLAN that you have specified in the VLAN field. If you have not selected the Use VLAN Interface check box, the IP address of the wireless controller's management VLAN is used.
Subnet Mask	Enter the subnet mask that is assigned to the wireless clients by the DHCP server.
Default Gateway	Enter the IP address of the default network gateway for all traffic beyond the local network.
Start IP	Enter the start IP address of the range that the DHCP server can assign.
End IP	Enter the end IP address of the range that the DHCP server can assign.
Use Default DNS Server	Select this check box to allow the DHCP server to use the wireless controller's default DNS servers. The Primary DNS Server and Secondary DNS Server fields are masked out.
Primary DNS Server	Enter the IP address of the primary DNS server for the network.

Setting	Description
Secondary DNS Server	Enter the IP address of the secondary DNS server for the network.
Use Default WINS Server	Select this check box to allow the DHCP server to use the wireless controller's default WINS server. The WINS Server field is masked out.
WINS Server	Enter the IP address of the WINS server for the network.

4. Click **Add**.

   The new DHCP server is added to the DHCP Server List.

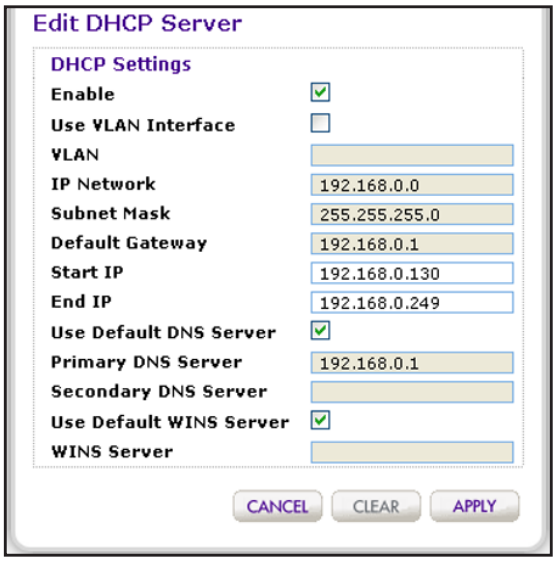
➢ **To edit a DHCP server:**

1. Select **Configuration > System > DHCP Server**.

   The DHCP Server List screen displays.

2. Select the radio button in the Edit/Remove column that corresponds to the DHCP server that you want to edit.
3. Click **Edit**.

   The Edit DHCP Server pop-up screen displays:



4. Make your changes (see the previous table).
5. Click **Apply**.

➢ **To delete a DHCP server:**

1. Select **Configuration > System > DHCP Server**.

   The DHCP Server List screen displays.

2. Select the radio button in the Edit/Remove column that corresponds to the DHCP server that you want to remove.
3. Click **Remove**.

Register Your Licenses

Make sure that your licenses cover the number of access points in your network. Before you can register your licenses, you need to configure the license server settings.

Note: When you install your licenses, they replace the default trial license for five access points.

For more information about licenses, see *Licenses* on page 18 and *Manage Licenses* on page 165.

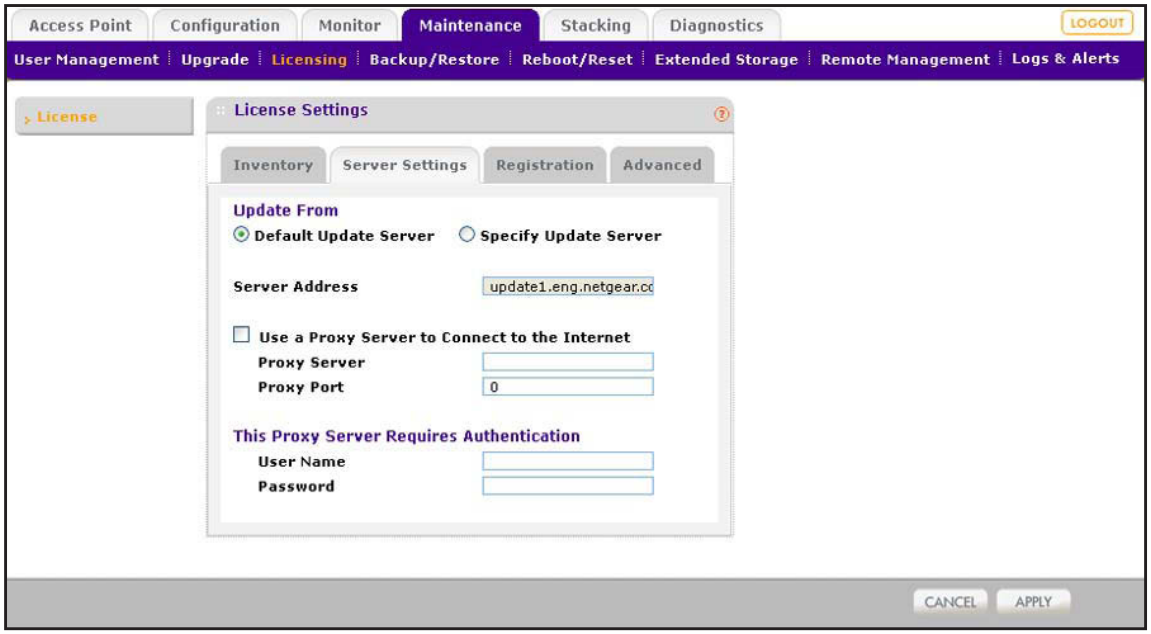
Configure the License Server Settings

Although you generally do not need to change the default license update server, you need to make sure that the wireless controller can reach the license update server.

➢ **To configure the license server settings:**

1. Select **Maintenance > License**.
2. Click the **Server Settings** tab.

   The Server Settings screen displays:



3. Configure the settings as described in the following table:

Setting	Description	
Update From	Select one of the following radio buttons to specify the license update server: • **Default Update Server**. The default license update server is used. • **Specify Update Server**. You need to specify the license update server. Fill in the Server Address field.	
	Server Address	Enter the IP address or FQDN of the server from which you import your licenses. By default, the FQDN of the NETGEAR license server is update1.eng.netgear.com.
Use a Proxy Server to Connect to the Internet	Select this check box if you use a proxy server to connect to the Internet.	
	Proxy Server	Enter the IP address or FQDN of the proxy server.
	Proxy Port	Enter the port that the proxy server uses.
This Proxy Server Requires Authentication	If the proxy server requires authentication, specify the user name and password.	
	User Name	Enter the user name to access the proxy server.
	Password	Enter the password to access the proxy server.

4. Click **Apply**.

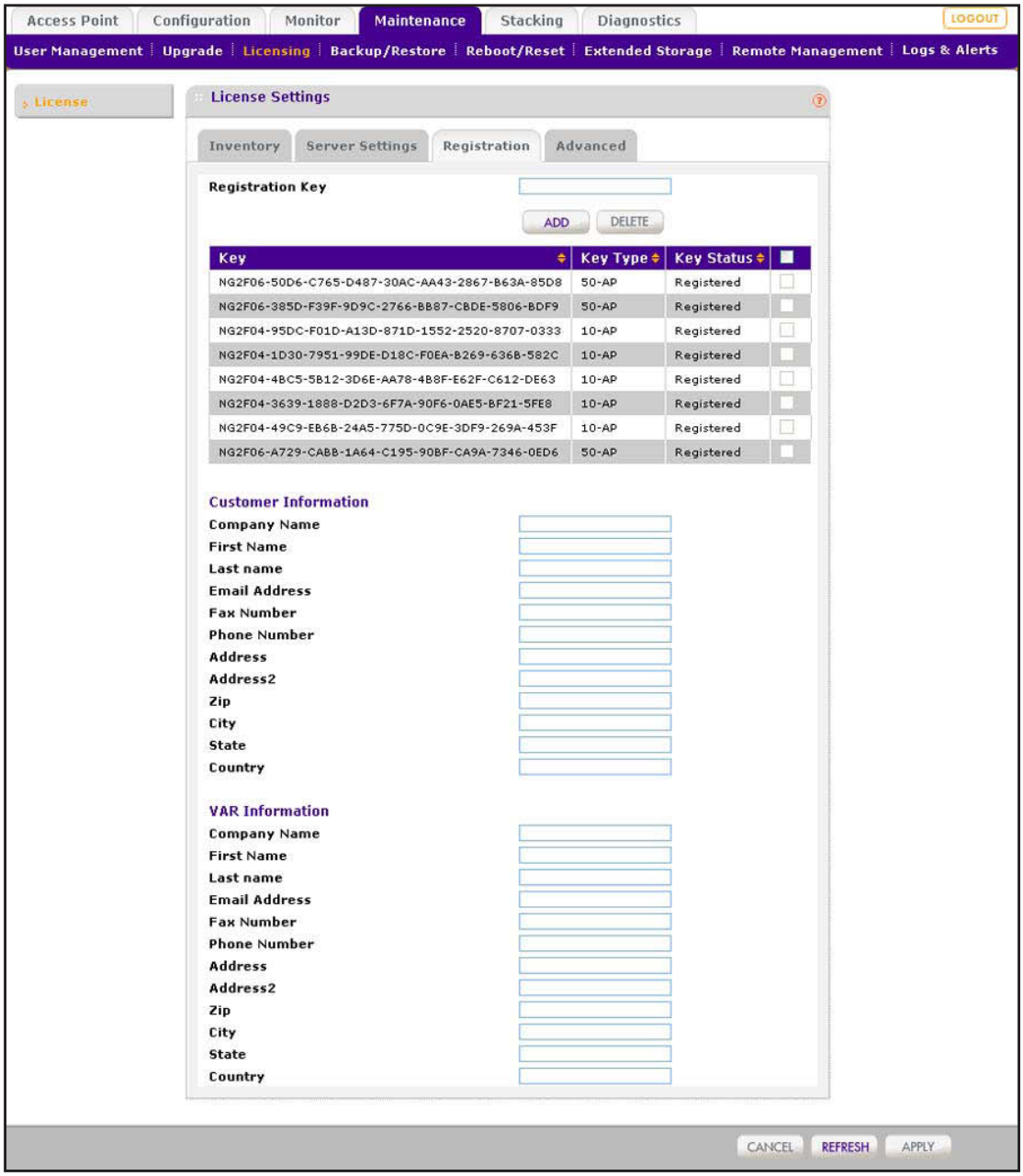
Register Your Licenses with the License Server

You need to have purchased licenses before you can register them. For more information, see *Licenses* on page 18)

➢ **To register your licenses:**

1. Make sure that the wireless controller is connected to the Internet.
2. Select **Maintenance > License**.
3. Click the **Registration** tab.

The Registration screen displays. The following figure shows some licenses already registered and installed. If you register licenses for the first time, the screen does not yet show any licenses.



4. Complete the Customer Information fields with the customer information that is associated with the key that you want to add and register.

   These fields are self-explanatory.

5. Complete the VAR Information fields with the value-added reseller (VAR) information that is associated with the key that you want to add and register.

   These fields are self-explanatory.

6. In the Registration Key field at the top of the screen, enter the registration key for the license that you want to add and register.
7. Click **Add**.

   The license is added to the table. The key details have the same meaning as those shown on the Inventory screen (see the Key Details section in the table in *View Your Licenses* on page 165).
8. Click **Apply**.

   Your license is registered.
9. (Optional) Repeat these steps to register another license.

The wireless controller lets you remove license keys that are invalid or that did not register successfully with the license server. However, you cannot remove licenses that registered successfully with the license server.

➢ **To remove a license:**

1. Select **Maintenance > License**.
2. Click the **Registration** tab.

   The Registration screen displays.
3. In the table, select the radio button that corresponds to the license that you want to remove.
4. Click **Delete**.

Manage Certificates

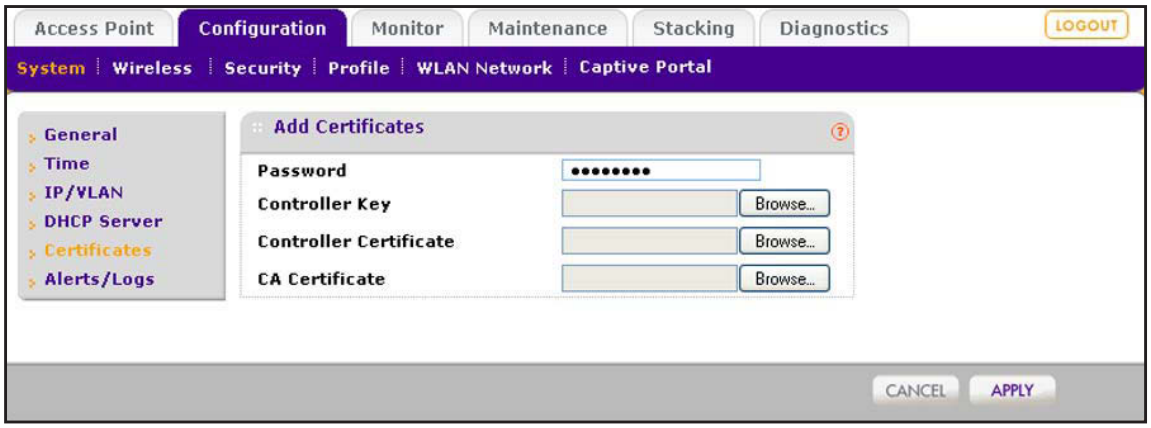
The internal authentication server for certificate-based authentication requires you to install a certificate on the wireless controller. A default self-signed server certificate is installed on the wireless controller. However, NETGEAR strongly recommends that you replace this default certificate with a custom certificate issued for your site or domain by a trusted certificate authority (CA).

To obtain a security certificate for the wireless controller, generate and submit a certificate signing request (CSR) to the CA of your choice. Upon receiving the CA-signed server certificate, install the certificate from your computer as described in this section. Certificates need to be in X.509 PEM format.

➢ **To add certificates:**

1. Select **Configuration > System > Certificates**.

The Add Certificates screen displays:



2. Configure the settings as described in the following table:

Setting	Description
Password	Enter the password for wireless controller certificates.
Controller Key	Click **Browse**, and select the controller key.
Controller Certificate	Click **Browse**, and select the controller certificate.
CA Certificate	Click **Browse**, and select the CA certificate.

3. Click **Apply**.

Configure Log, Syslog, Alarm Notification, and Email Settings

From the Alerts/Logs menu you can configure the logs, syslog, and the alarms, and specify the email address from which alerts originate.

Configure Log Settings

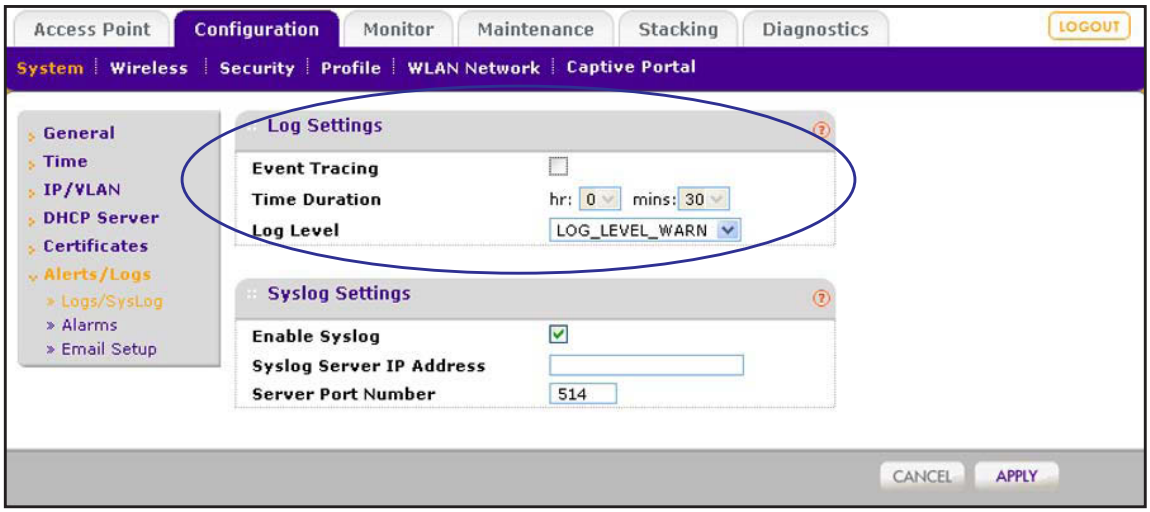
For the logs, you can either configure event tracing or select a log level. These selections are mutually exclusive.

Event tracing can help you to debug the wireless network. Event tracing generates logs from the wireless controller and from all controlled access points, and saves these logs in a file on the wireless controller. The file can become large quickly.

➢ **To configure the log settings and view the logs:**

1. Select **Configuration > System > Alerts/Logs > Logs/Syslog**.

The Logs Settings screen displays:



2. In the Logs Settings section of the screen, configure either event tracing or a log level (these selections are mutually exclusive):
   - **Event tracing**. To configure event tracing:
     a. Select the **Event Tracing** check box.
     b. Next to Time Duration, use the menus to specify the period during which event tracing should occur.
   - **Log level**. From the Log Level menu, select one of the following levels:
     - **LOG_LEVEL_CRIT**. Critical errors only are logged.
     - **LOG_LEVEL_ERR**. Noncritical errors and critical errors are logged.
     - **LOG_LEVEL_WARN**. Warnings, noncritical errors, and critical errors are logged.
     - **LOG_LEVEL_NOTICE**. Notifications, warnings, noncritical errors, and critical errors are logged.
     - **LOG_LEVEL_INFO**. Informational messages, notifications, warnings, noncritical errors, and critical errors are logged.
3. Click **Apply**.

For information about saving and clearing the logs, see *View Alerts and Events and Save the Logs* on page 159.

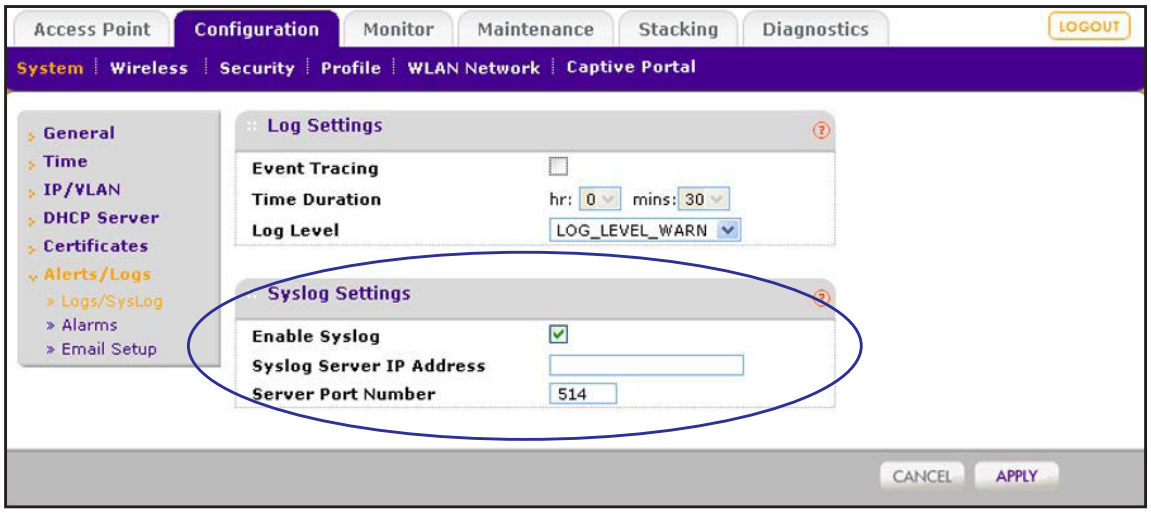
Configure Syslog Settings

This screen lets you configure the settings to connect to a syslog server, if you have one configured in your network.

➢ **To configure syslog settings:**

1. Select **Configuration > System > Alerts/Logs > Logs/Syslog**.

   The Logs Settings screen displays:



2. In the Syslog Settings section of the screen, configure the settings as described in the following table:

Setting	Description
Enable Syslog	Enable the syslog settings, if you have a syslog server on your network.
Syslog Server IP Address	Enter the IP address to which the wireless controller and managed access points send all syslogs, if the Syslog check box is selected.
Server Port Number	Enter the number of the port at which your syslog server is configured to listen to requests.

3. Click **Apply**.

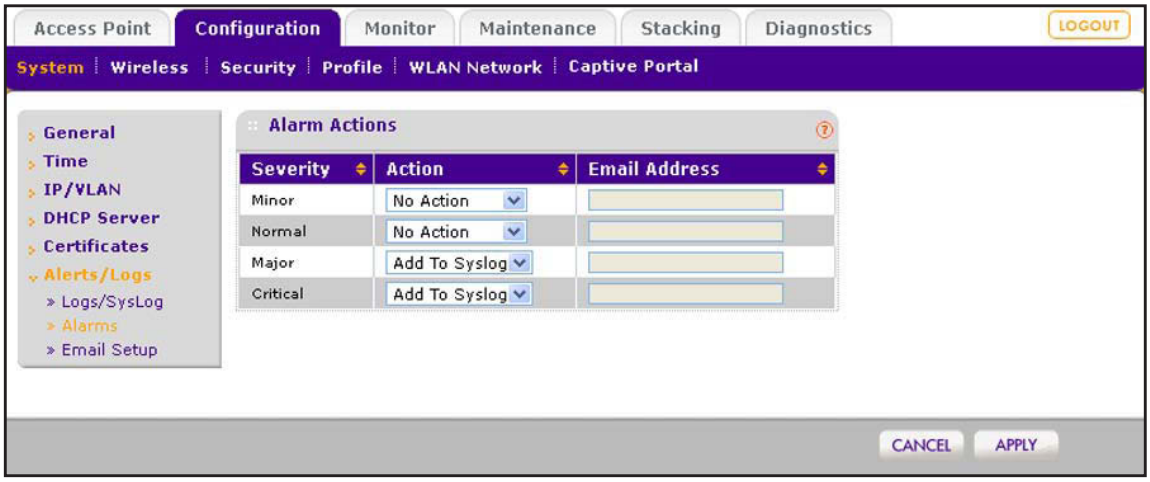
Configure Alarm Notification Settings

You can classify certain events as critical, major, normal, or minor. Some events you can classify only as critical or major. For example, on the RF Management screen, you can specify whether a coverage hole should be classified as critical or major (see *RF Management for the Basic Profile Group* on page 141).

➢ **To configure alarm actions:**

1. Select **Configuration > System > Alerts/Logs > Alarms**.

   The Alarm Actions screen displays:



2. For each alarm severity (Minor, Normal, Major, and Critical), select the desired action from its corresponding Action menu.
   - **No Action**. When the alarm occurs, no action is taken.
   - **Add To Syslog**. When the alarm occurs, the wireless controller adds an entry to the syslog.
   - **Send Email**. When the alarm occurs, the wireless controller sends an email.
3. For each alarm severity for which you have selected the Send Email option in the previous step, enter an email address.
4. Click **Apply**.

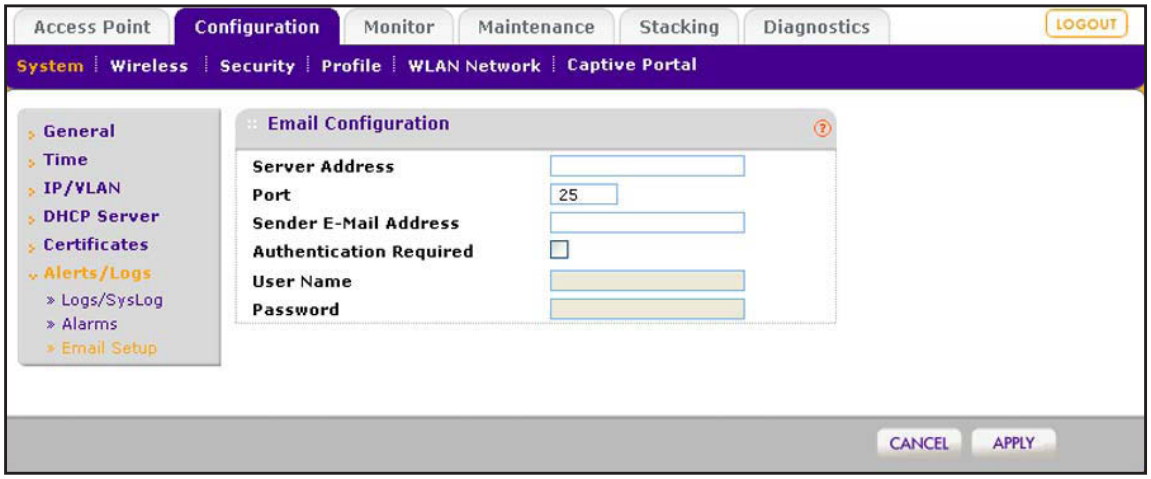
Configure the Email Notification Server

The email notification server is the location from which the email alerts originate.

➢ **To configure email settings:**

1. Select **Configuration > System > Alerts/Logs > Email Setup**.

   The Email Configuration screen displays:



2. Configure the settings as described in the following table:

Setting	Description	
Server Address	Enter the IP address of the server from which email notifications are sent.	
Port	Enter the port number of the server from which email notifications are sent. The default is port number 25.	
Sender Email Address	Enter the email address from which email notifications are sent.	
Authentication Required	Select this check box if the email server requires authentication, and complete the User Name and Password fields.	
	User Name	Enter the user name that is associated with the email server.
	Password	Enter the password that is associated with the email server.

3. Click **Apply**.

Manage Security Profiles and Profile Groups

5

This chapter includes the following sections:

- *Wireless Security Profile Concepts*
- *Configure Security Profiles for the Basic Profile Group*
- *Configure Security Profiles for Advanced Profile Groups*
- *Network Authentication and Data Encryption Options*
- *Manage MAC Authentication and MAC Authentication Groups*
- *Manage Authentication Servers and Authentication Server Groups*

Note: In this chapter and in the following chapters, access point profile groups are referred to as just profile groups.
Profiles, security profiles, and SSIDs (that is, SSIDs with associated security settings) are terms that are interchangeable.

Wireless Security Profile Concepts

Profiles are sets of configurations that you can apply to an access point. The configuration includes radio parameters, load-balancing parameters, and rate-limit parameters. Each wireless radio on an access point can support eight profiles. This means that the dual-band WNDAP350 access point can support a total of 16 profiles. Therefore, in one profile group on the wireless controller, you can configure up to eight profiles for each radio, that is, up to eight profiles for the 2.4 GHz radio *and* up to eight profiles for the 5 GHz radio.

Setting up profiles allows you to configure the WLAN network offline. Then, when the WLAN network is operating, you can push the configuration onto managed access points. You can configure profiles and profile groups without taking the state of the access points into consideration. When the access points connect to the wireless controller, the profile configurations are pushed onto the access points.

Note: If an access point is removed from its building (someone takes it home or it is stolen), the access point does not retain the configuration that it received from the wireless controller. The configuration is not stored in memory on the access point.

Depending on your network needs, you can either use the basic profile group (that is, the basic configuration) or the advanced profile groups (that is, the advanced configuration). The basic profile group works well for small-scale WLAN networks; advanced profile groups are useful for larger deployments.

Note: For more information about basic and advanced profile groups, see *Basic and Advanced Setting Concepts* on page 20.

Small WLAN Networks

For small WLAN networks, you can use the basic configuration with the basic profile group. All access points belong to the same group and use the same wireless, security, and QoS configurations.

The basic profile group can contain up to 16 profiles for a dual-band access point, or eight profiles for a single-band access point. Each profile has its own SSID and can have its own VLAN to allow the profile to establish its own tunnel. Profiles can also share the same VLAN.

For example, in an enterprise network in which all access points managed by the wireless controller serve the same wireless networks and have the same settings, you can use the basic configuration.

Larger WLAN Networks

For larger network deployments that consist of different sets of WLAN networks, consider using the advanced configuration to create multiple profile groups. The access points that belong to the same profile group use the same wireless, security, and QoS configurations.

The wireless controller supports up to eight profile groups. Each profile group can have its own wireless, security, and QoS configurations. Each profile group can contain up to 16 profiles for a dual-band access point, or eight profiles for a single-band access point. Using dual-band access points, the wireless controller could support a total of 128 profiles. Each profile has its own SSID and can have its own VLAN to allow the profile to establish its own tunnel. Profiles can also share the same VLAN.

In larger network deployments also, you would assign guests to a separate VLAN because guests typically access only the Internet, not the business network, and do not have peer-to-peer access.

Profile Naming Conventions

You can use profile naming conventions that are based on user groups such as Marketing, or based on VLANs such as VLAN40, or you can use other naming conventions such as CompanyName15.

Note: In the advanced configuration, you cannot change the names of profile groups. However, you can change the group names of MAC ACLs and external RADIUS servers.

Considerations Before You Configure Profiles

Before you create and configure profiles for the basic profile group or an advanced profile group, consider the following:

- **Authentication servers**. If you want to use external LDAP or RADIUS authentication, or both, first configure the authentication server settings:
  - Configure basic server settings on the basic Authentication Server screen (see *Configure Basic Authentication Server Settings* on page 86).
  - For more complex networks, configure additional RADIUS servers on the advanced Authentication Server screen (see *Configure RADIUS Authentication Server Groups* on page 88).

  After you have configured authentication server settings, you can then assign any authentication server to a security profile in a basic profile group or advanced profile group.

Note: You can configure profiles to function with different authentication servers. For example, you could set up a guest profile with no authentication, an engineering profile that uses external RADIUS authentication, and a marketing profile that uses external LDAP authentication. You can also use additional external RADIUS servers in other profiles.

- **MAC authentication**. If you want to use a MAC access control list (ACL) to control access of wireless clients, first create one or more MAC ACLs:
  - Configure the basic MAC ACL on the basic MAC Authentication screen (see *Configure Basic Local MAC Authentication Settings* on page 82).
  - For more complex networks, configure additional MAC ACLs on the advanced MAC Authentication screen (see *Configure Local MAC Authentication Groups* on page 84).

  After you have configured one or more MAC ACLs, you can then assign any MAC ACL to a security profile in a basic profile group or advanced profile group.
- **Cloning profiles**. For faster setup, you can clone a profile and rename it. Cloning copies all settings except for the name and SSID.

Basic and Advanced Security Configuration Concepts

The basic security configuration model (Configuration > Security > Basic) does not apply strictly to the basic profile group, nor does the advanced security configuration model (Configuration > Security > Advanced) apply strictly to advanced profile groups. The reason is that you apply an authentication server and a MAC ACL to an individual profile and not to a profile group.

- **Basic security settings**. You can apply the following security settings to *any* profile, whether in the basic profile group or in an advanced profile group:
  - Basic MAC authentication (the MAC ACL group that is called basic)
  - Basic authentication server (the RADIUS server that is called basic-Auth or the LDAP server that is called basic-LDAP)
- **Advanced security settings**. You can apply the following security settings to *any* profile, whether in the basic profile group or in an advanced profile group:
  - Advanced MAC authentication (the MAC ACLs that are, by default, called Acl-1, Acl-2, Acl-3, and so on; you can change these default names)
  - Advanced authentication server (the RADIUS servers that are, by default, called Auth-1, Auth-2, Auth-3, and so on; you can change these default names)

Configure Security Profiles for the Basic Profile Group

The basic profile group works well for small-scale WLAN networks. NETGEAR recommends that you read the information in the previous section, *Wireless Security Profile Concepts*, before you configure any profiles.

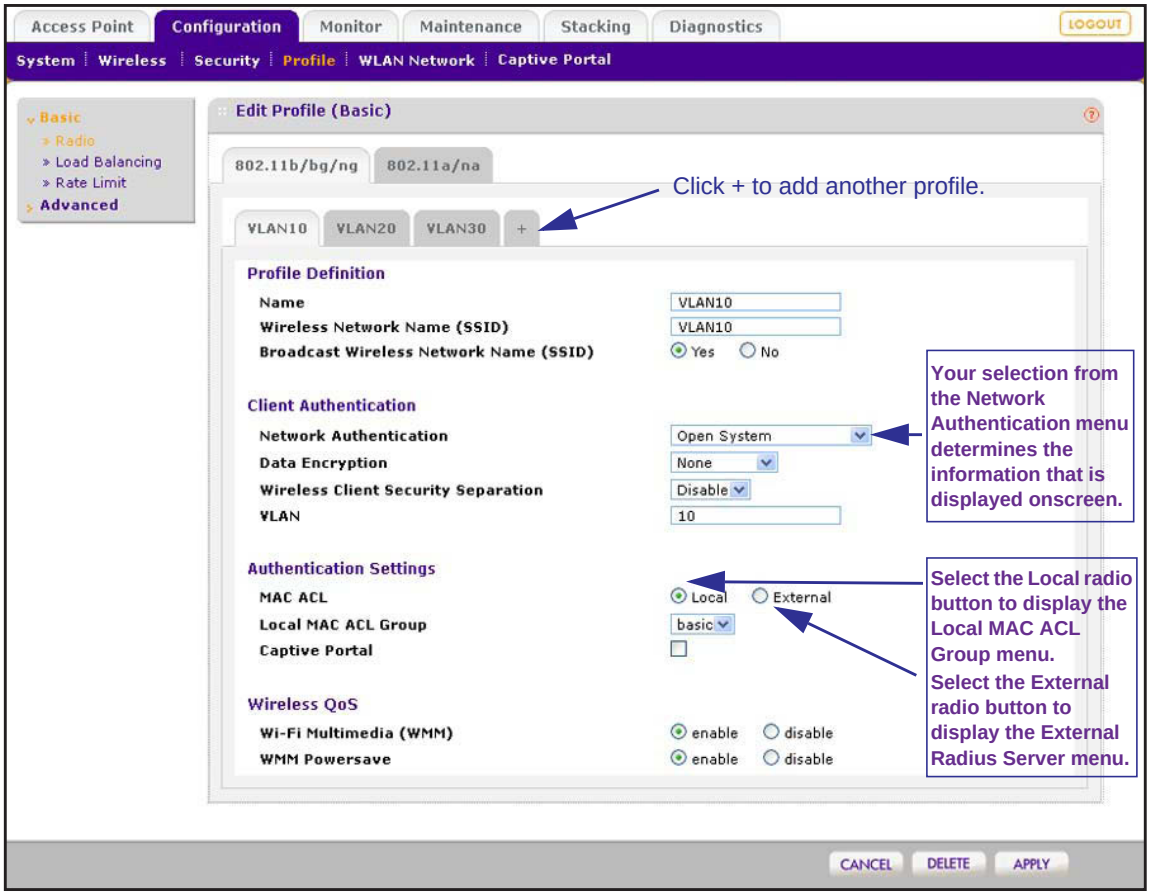
Configure Profiles in the Basic Profile Group

The Edit Profile (Basic) screen lets you create and configure up to eight security profiles per wireless radio (eight profiles for a single-band access point; 16 profiles for a dual-band access point). Separate profiles are applied to 802.11b/bg/ng-mode and 802.11a/na-mode radios.

➢ **To add a security profile to the basic profile group and configure the security profile:**

1. Select **Configuration > Profile > Basic > Radio**.

   The Edit Profile (Basic) screen displays:



   By default, an NG_11g profile and an NG_11a profile are present in the basic profile group.

2. Click the tab for the radio for which you want to add a profile.

3. Click the **+** button to add the profile to the basic profile group.

   The Add Profiles pop-up screen displays.

4. (Optional) Clone an existing profile:
   a. Select the **Clone an existing Profile** check box.

      The previous figure shows that you can clone an existing profile with the name VLAN10.

   b. Select a profile from the Profiles menu.
5. Click **Add**.

The newly created profile displays onscreen, and the tab for the new profile is automatically selected to let you configure the new profile.

Note: The selections that are available from the Network Authentication menu are affected by the authentication server settings that you specify on the Authentication Server screen. For more information, see *Manage Authentication Servers and Authentication Server Groups* on page 85. If your selection from the Network Authentication menu requires authentication, a corresponding Authentication Server field displays.

6. Configure the settings as described in the following table:

Setting	Description
Profile Definition section	
Name	Enter a unique name to identify the profile. This value can be up to 32 alphanumeric characters. Use meaningful profile names instead of the default names. The default profile names are Profile1, Profile2, and so on, through Profile8.
Wireless Network Name (SSID)	Enter a unique name for the wireless network associated with this profile.

Setting	Description	
Broadcast Wireless Network Name	Select the **Yes** radio button to enable broadcast of the SSID. This is the default setting. Select the **No** radio button to disable broadcast of the SSID, in which case only devices that have the correct SSID can connect to the access point.	
Client Authentication section **Note:** The options that display onscreen depend on your selection from Network Authentication menu.		
Network Authentication	From the menu, select the authentication type to be used. *Table 3* on page 78 lists all the authentication type options.	
Data Encryption	From the menu, select the data encryption type to be used. The options available for data encryption as well as other requirements such as entering a key or passphrase depend on the network authentication settings. *Table 3* on page 78 lists all the data encryption options.	
Wireless Client Security Separation	From the menu, select **Disable** to prevent associated wireless clients from communicating with each other, or select **Enable** to allow such communication. Wireless client separation is intended for hotspots and other public access situations.	
VLAN	Enter the VLAN ID to be associated with this security profile. This VLAN ID needs to match the VLAN ID that is used by other network devices.	
Authentication Settings section **Note:** The options that display onscreen depend on the selection from Network Authentication menu.		
Note: MAC ACL displays only when you select Open System, Shared Key, WPA-PSK, WPA2-PSK, or WPA-PSK & WPA2-PSK from the Network Authentication menu.	MAC ACL	Select one of the following radio buttons: • **Local**. Use local MAC authentication. The Local MAC ACL Group menu displays so you can select a group. For more information, see *Manage MAC Authentication and MAC Authentication Groups* on page 81. • **External**. Use external MAC authentication. The External Radius Server menu displays so you can select a server. You can use either the basic-Auth RADIUS server or a RADIUS server of an advanced authentication group. You cannot use the external LDAP server. For information about setting up and enabling internal and external authentication servers, see *Manage Authentication Servers and Authentication Server Groups* on page 85. **Note:** The MAC ACL radio buttons do not display onscreen if the network authentication uses an external RADIUS server. The reason for this is that you can configure either MAC authentication with an external RADIUS server or network authentication with an external RADIUS server, but not both. That is, if you configure an external RADIUS server with WPA, WPA2, or WPA & WPA2 (or you use Legacy 802.1X), you cannot use external MAC authentication, and the MAC ACL radio buttons do not display on screen. You can still use internal MAC authentication.

Setting	Description	
Note: Captive Portal displays only when you select Open System, Shared Key, WPA-PSK, WPA2-PSK, or WPA-PSK & WPA2-PSK from the Network Authentication menu.	Captive Portal	Select this check box if you want to enable the captive portal. For more information, see *Manage Guest Network Access* on page 111. **Note:** You cannot configure captive portal authentication if the network authentication uses a RADIUS server, whether it is a local server or an external server. That is, if you configure a RADIUS server with WPA, WPA2, or WPA & WPA2 (or if you use legacy 802.1X), the Captive Portal check box is not shown onscreen.
Note: Authentication Server displays only when you select WPA with Radius, WPA2 with Radius, or WPA & WPA2 with Radius from the Network Authentication menu.	Authentication Server	Select one of the following radio buttons: • **Local**. Use the local authentication server. • **External**. Use an external authentication server. Select an external authentication server from the Authentication Server menu. **Note:** For information about setting up and enabling internal and external authentication servers, see *Manage Authentication Servers and Authentication Server Groups* on page 85.
Wireless QoS section		
Wi-Fi Multimedia (WMM)	To enable Wi-Fi Multimedia (WMM), select the **Enable** radio button, which is the default setting. Select the **Disable** button to disable the feature. For more information, see *Configure QoS for Advanced Profile Groups* on page 144.	
WMM Powersave	The WMM Powersave feature saves power for battery-powered equipment by increasing the efficiency and flexibility of data transmission. To enable this feature, select the **Enable** radio button, which is the default setting. Select the **Disable** button to disable the feature.	

7. Click **Apply**.

Edit and Remove Profiles in the Basic Profile Group

You can easily change or remove a profile from the basic profile group.

➢ **To edit an existing profile:**

1. Select **Configuration > Profile > Basic > Radio**.

   The Edit Profile (Basic) screen displays.

2. Click the tab for the radio for which you want to edit a profile.
3. Click the tab for the profile that you want to edit.
4. Change the settings.

   For information about how to change the settings, see *Configure Profiles in the Basic Profile Group* on page 67.

5. Click **Apply**.

➢ **To remove an existing profile:**

1. Select **Configuration > Profile > Basic > Radio**.

   The Edit Profile (Basic) screen displays.

2. Click the tab for the radio for which you want to remove a profile.
3. Click the tab for the profile that you want to remove.
4. Click **Delete**.
5. Confirm that you want to delete the profile.

Configure Security Profiles for Advanced Profile Groups

Advanced profile groups are useful for larger deployments. NETGEAR recommends that you read the information in the *Wireless Security Profile Concepts* on page 64 before you configure any profile groups and profiles.

Advanced Profile Groups

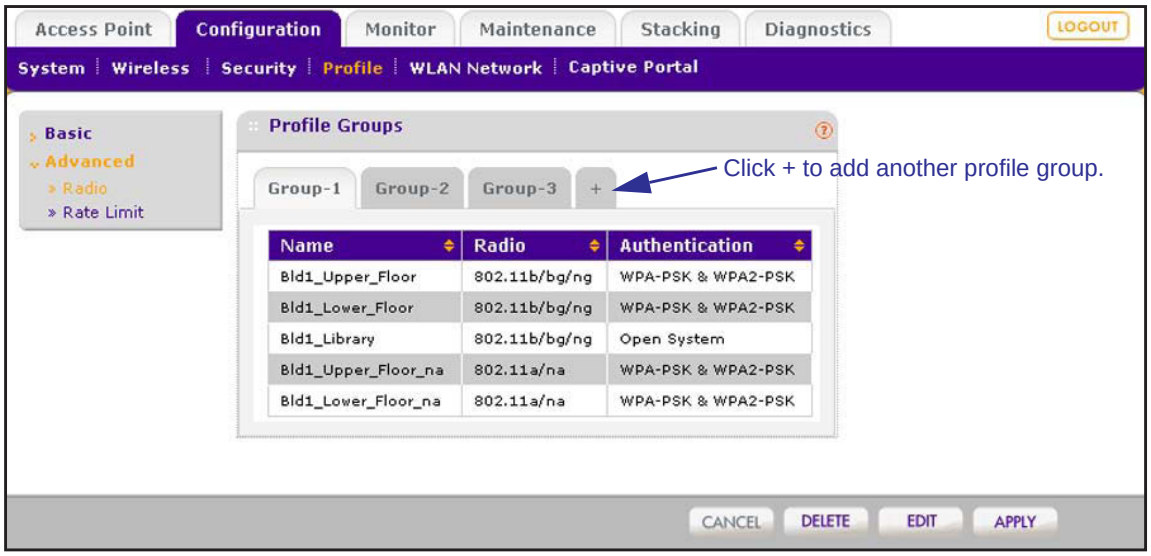
The advanced Profile Group screen lets you create up to eight profile groups. For each profile group, you can create and configure up to eight security profiles per wireless radio (eight profiles for a single-band access point; 16 profiles for a dual-band access point). Separate profiles are applied to 802.11b/bg/ng-mode and 802.11a/na-mode radios.

By default, all access points are assigned to the basic profile group. After you have created advanced profile groups, you can use the WLAN Network screen to reassign access points to any of these advanced profile groups (see *Assign Access Points to Advanced Profile Groups* on page 104).

➢ **To add an advanced profile group:**

1. Select **Configuration > Profile > Advanced > Radio**.

The Profile Groups screen displays:



2. To add a profile group, click the **+** button.

   The new profile group displays on the Profile Groups screen. By default, an NG_11g-0 profile and an NG_11a-0 profile are present in a profile group.

Note: By default, profile groups are named Group-1, Group-2, Group-3, and so on. You *cannot* change these profile group names.

The following table describes the fields that are shown for each profile in a profile group.

Setting	Description
Name	The unique profile name.
Radio	The wireless radio mode in which the profile is operating.
Authentication	The authentication setting under which the profile is operating.

➢ **To remove an advanced profile group:**

1. Select **Configuration > Profile > Advanced > Radio**.

   The Profile Groups screen displays.

2. Click the tab for the profile group that you want to remove.
3. Click **Delete**.

Note: There is no separate procedure to edit profile groups. You edit profile groups by adding, removing, or changing profiles in the profile group.

Configure Profiles in an Advanced Profile Group

For each profile group, the Edit Profile (Group-*X*) screen lets you create and configure up to eight security profiles per wireless radio (eight profiles for a single-band access point; 16 profiles for a dual-band access point). Separate profiles are applied to 802.11b/bg/ng-mode and 802.11a/na-mode radios.

➢ **To add a security profile to an advanced profile group and configure the security profile:**

1. Select **Configuration > Profile > Advanced > Radio**.

   The Profile Groups screen displays.

2. Click **Edit**.

   The Edit Profile (Group-*X*) screen displays.

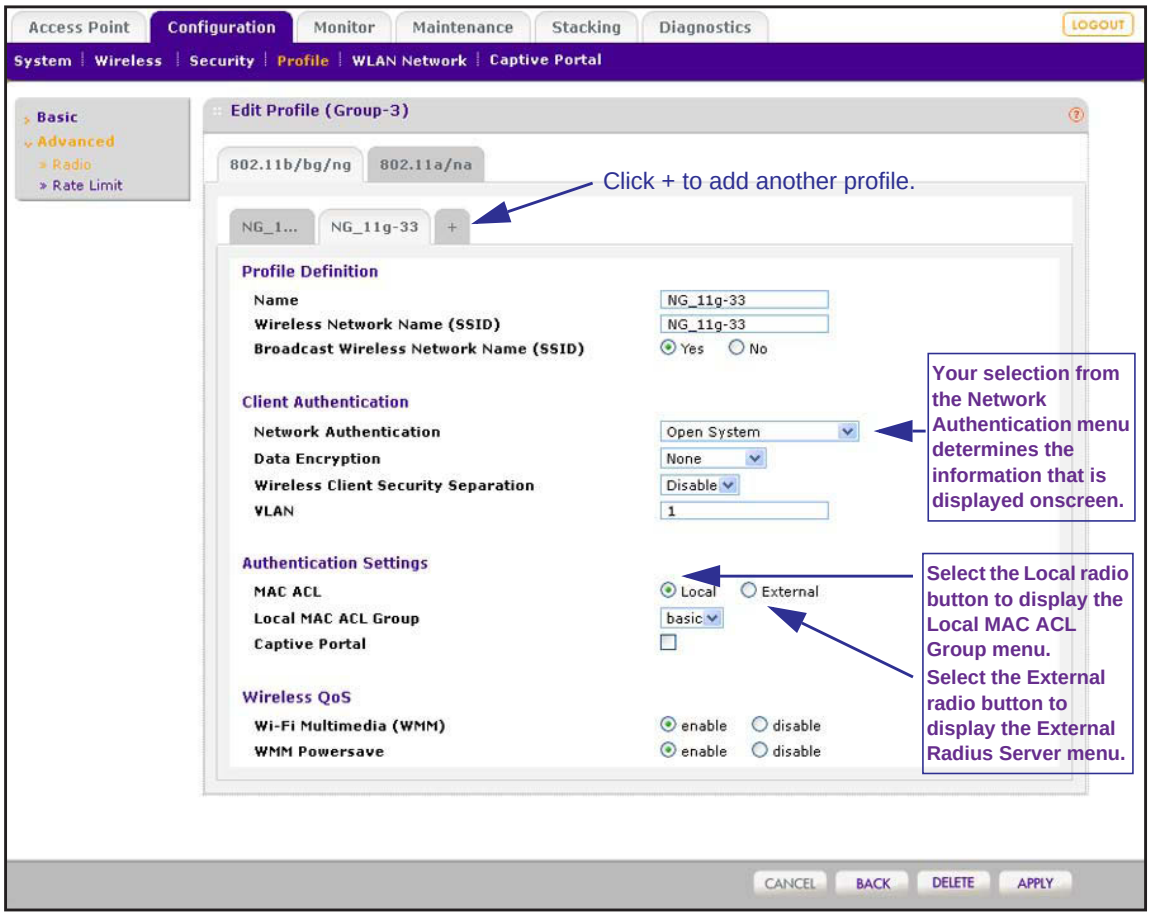
3. Click the tab for the radio that for which you want to add a profile.
4. Click the **+** button to add the profile to the selected advanced profile group.

   The Add Profiles pop-up screen displays:

5. (Optional) Clone an existing profile:
   a. Select the **Clone an existing Profile** check box.
   b. Select a profile from the Profiles menu.
6. Click **Add**.

   The newly created profile displays onscreen, and the tab for the new profile is automatically selected to let you configure the new profile.

Note: The selections that are available from the Network Authentication menu are affected by the authentication server settings that you specify on the Authentication Server screen. For more information, see *Manage Authentication Servers and Authentication Server Groups* on page 85. If your selection from the Network Authentication menu requires authentication, a corresponding Authentication Server field displays.



7. Configure the settings as described in the following table:

Setting	Description
Profile Definition section	
Name	Enter a unique name to identify the profile. This value can be up to 32 alphanumeric characters. Use meaningful profile names instead of the default names. The default profile names are Profile1, Profile2, and so on, through Profile8.
Wireless Network Name (SSID)	Enter a unique name for the wireless network associated with this profile.
Broadcast Wireless Network Name	Select the **Yes** radio button to enable broadcast of the SSID. This is the default setting. Select the **No** radio button to disable broadcast of the SSID, in which case only devices that have the correct SSID can connect to the access point.

Setting	Description	
Client Authentication section **Note:** The options that display onscreen depend on your selection from Network Authentication menu.		
Network Authentication	From the menu, select the authentication type to be used. *Table 3* on page 78 lists all the authentication type options.	
Data Encryption	From the menu, select the data encryption type to be used. The options available for data encryption as well as other requirements such as entering a key or passphrase depend on the network authentication settings. *Table 3* on page 78 lists all the data encryption options.	
Wireless Client Security Separation	From the menu, select **Disable** to prevent associated wireless clients from communicating with each other, or select **Enable** to allow such communication. Wireless client separation is intended for hotspots and other public access situations.	
VLAN	Enter the VLAN ID to be associated with this security profile. This VLAN ID needs to match the VLAN ID that is used by other network devices.	
Authentication Settings section **Note:** The options that display onscreen depend on the selection from Network Authentication menu.		
Note: MAC ACL displays only when you select Open System, Shared Key, WPA-PSK, WPA2-PSK, or WPA-PSK & WPA2-PSK from the Network Authentication menu.	MAC ACL	Select one of the following radio buttons: • **Local**. Use local MAC authentication. The Local MAC ACL Group menu displays so you can select a group. For more information, see *Manage MAC Authentication and MAC Authentication Groups* on page 81. • **External**. Use external MAC authentication. The External Radius Server menu displays so you can select a server. You can use either the basic-Auth RADIUS server or a RADIUS server of an advanced authentication group. You cannot use the external LDAP server. For information about setting up and enabling internal and external authentication servers, see *Manage Authentication Servers and Authentication Server Groups* on page 85. **Note:** The MAC ACL radio buttons do not display onscreen if the network authentication uses an external RADIUS server. The reason for this is that you can configure either MAC authentication with an external RADIUS server or network authentication with an external RADIUS server, but not both. That is, if you configure an external RADIUS server with WPA, WPA2, or WPA & WPA2 (or you use Legacy 802.1X), you cannot use external MAC authentication, and the MAC ACL radio buttons do not display on screen. You can still use internal MAC authentication.

Setting	Description	
Note: Captive Portal displays only when you select Open System, Shared Key, WPA-PSK, WPA2-PSK, or WPA-PSK & WPA2-PSK from the Network Authentication menu.	Captive Portal	Select this check box if you want to enable the captive portal. For more information, see *Manage Guest Network Access* on page 111. **Note:** You cannot configure captive portal authentication if the network authentication uses a RADIUS server, whether it is a local server or an external server. That is, if you configure a RADIUS server with WPA, WPA2, or WPA & WPA2 (or if you use legacy 802.1X), the Captive Portal check box is not shown onscreen.
Note: Authentication Server displays only when you select WPA with Radius, WPA2 with Radius, or WPA & WPA2 with Radius from the Network Authentication menu.	Authentication Server	Select one of the following radio buttons: • **Local**. Use the local authentication server. • **External**. Use an external authentication server. Select an external authentication server from the Authentication Server menu. **Note:** For information about setting up and enabling internal and external authentication servers, see *Manage Authentication Servers and Authentication Server Groups* on page 85.
Wireless QoS section		
Wi-Fi Multimedia (WMM)	To enable Wi-Fi Multimedia (WMM), select the **Enable** radio button, which is the default setting. Select the **Disable** button to disable the feature. For more information, see *Configure QoS for Advanced Profile Groups* on page 144.	
WMM Powersave	The WMM Powersave feature saves power for battery-powered equipment by increasing the efficiency and flexibility of data transmission. To enable this feature, select the **Enable** radio button, which is the default setting. Select the **Disable** button to disable the feature.	

8. Click **Apply**.

Edit and Remove Profiles in an Advanced Profile Group

You can easily change or remove a profile from an advanced profile group.

➢ **To edit an existing profile to an advanced profile group:**

1. Select **Configuration > Profile > Advanced > Radio**.

   The Profile Groups screen displays.

2. Click the tab for the profile group for which you want to edit a profile.
3. Click **Edit**.

   The Edit Profile screen displays.

4. Click the tab for the radio for which you want to edit a profile.

5. Click the tab for the profile that you want to edit.
6. Change the settings.

   For information about how to change the settings, see *Configure Profiles in an Advanced Profile Group* on page 73.
7. Click **Apply**.

➢ **To remove an existing profile from an advanced profile group:**

1. Select **Configuration > Profile > Advanced > Radio**.

   The Profile Groups screen displays.
2. Click the tab for the profile group for which you want to remove a profile.
3. Click **Edit**.

   The Edit Profile (Group-*X*) screen displays.
4. Click the tab for the radio for which you want to remove a profile.
5. Click the tab for the profile that you want to remove.
6. Click **Delete**.
7. Confirm that you want to delete the profile.

Network Authentication and Data Encryption Options

This section describes the detailed network authentication and data encryption options that are part of the procedures in *Configure Profiles in the Basic Profile Group* on page 67 and *Configure Profiles in an Advanced Profile Group* on page 73.

Table 3 on page 78 shows the data encryption options based on the network authentication that you select on the Edit Profile (Basic) or Edit Profile (Group-*X*) screen, and the required configuration steps to implement the selected network authentication.

Note: On the Edit Profile (Basic) or Edit Profile (Group-*X*) screen, for any selection from the Network Authentication menu that requires a RADIUS server, authentication is not restricted to a RADIUS server; you can also use an internal authentication server or an external LDAP server.

Note: You can configure either MAC authentication with an external RADIUS server or network authentication with an external RADIUS server, but not both. That is, if you configure external MAC authentication, you cannot use an external RADIUS server with WPA, WPA2, or WPA & WPA2.

Table 3. Network authentication and data encryption settings

Network Authentication Selection	Data Encryption Options	Configuration Steps
Open	None WEP	You can use an open system without any encryption or with WEP encryption: • **No encryption**. An open system without encryption is the default setting. No further authentication and encryption configuration is required. • **WEP encryption**. To configure an open system with WEP encryption, see the Shared Key and WEP information further down in this table.
Shared Key	64-bit WEP 128-bit WEP 152-bit WEP	To configure Shared Key authentication with WEP: 1. From the Data Encryption menu, select a level of WEP encryption: - **64-bit WEP**. Uses 40/64-bit encryption. - **128-bit WEP**. Uses 104/128-bit encryption. - **152-bit WEP**. A proprietary mode that works only with other wireless devices that support this mode. 2. (Optional) Select the **Show Key** check box to display the characters in the key fields. 3. Select a key radio button (**Key1**, **Key2**, **Key3**, or **Key4**). 4. Enter a key in the corresponding field: - 64-bit WEP requires a key with 10 characters. - 128-bit WEP requires a key with 26 characters. - 152-bit WEP requires a key with 32 characters. **Note:** For information about requirements for WEP keys, see *Table 6* on page 207.
Legacy 802.1x	None	To configure legacy 802.1x authentication: 1. Set up and enable an internal or external (RADIUS or LDAP) authentication server. For information, see *Manage Authentication Servers and Authentication Server Groups* on page 85. 2. Select the **Local** or **External** radio button. 3. If you select the External radio button, select the authentication server that you wish to use from the menu.

Table 3. Network authentication and data encryption settings (continued)

Network Authentication Selection	Data Encryption Options	Configuration Steps
WPA with Radius	TKIP TKIP + AES	To configure WPA authentication with a RADIUS server: 1. Set up and enable an internal or external (RADIUS or LDAP) authentication server. For information, see *Manage Authentication Servers and Authentication Server Groups* on page 85. 2. From the Data Encryption menu, select the type of encryption: - **TKIP**. Supports Temporal Key Integrity Protocol (TKIP) only. - **TKIP + AES**. Supports both TKIP and Advanced Encryption Standard (AES). 3. Select the **Local** or **External** radio button. 4. If you select the External radio button, select the authentication server that you wish to use from the menu.
WPA2 with Radius	AES TKIP + AES	To configure WPA2 authentication with a RADIUS server: 1. Set up and enable an internal or external (RADIUS or LDAP) authentication server. For information, see *Manage Authentication Servers and Authentication Server Groups* on page 85. 2. From the Data Encryption menu, select the type of encryption: - **AES**. Supports AES only. - **TKIP + AES**. Supports both TKIP and AES. 3. Select the **Local** or **External** radio button. 4. If you select the External radio button, select the authentication server that you wish to use from the menu.
WPA & WPA2 with Radius **Note:** Use this option if there are both WPA and WPA2 clients in the network.	TKIP + AES	To configure WPA & WPA2 authentication with a RADIUS server: 1. Set up and enable an internal or external (RADIUS or LDAP) authentication server. For information, see *Manage Authentication Servers and Authentication Server Groups* on page 85. 2. Select the **Local** or **External** radio button. 3. If you select the External radio button, select the authentication server that you wish to use from the menu. **Note:** The Data Encryption menu displays TKIP + AES, which is the only available option. Both TKIP and AES are supported.

Table 3. Network authentication and data encryption settings (continued)

Network Authentication Selection	Data Encryption Options	Configuration Steps
WPA-PSK	TKIP TKIP + AES	To configure WPA-PSK authentication: 1. From the Data Encryption menu, select the type of encryption: - **TKIP**. Supports TKIP only. - **TKIP + AES**. Supports both TKIP and AES. 2. (Optional) Select the **Show Passphrase** check box to display the characters in the WPA Passphrase (Network Key) field. 3. Type a passphrase of at least eight characters in the WPA Passphrase (Network Key) field. **Note:** For information about requirements for a WPA passphrase, see *Table 6* on page 207.
WPA2-PSK	AES TKIP + AES	To configure WPA2-PSK authentication: 1. From the Data Encryption menu, select the type of encryption: - **AES**. Supports AES only. - **TKIP + AES**. Supports both TKIP and AES. 2. (Optional) Select the **Show Passphrase** check box to display the characters in the WPA Passphrase (Network Key) field. 3. Type a passphrase of at least eight characters in the WPA Passphrase (Network Key) field. **Note:** For information about requirements for a WPA passphrase, see *Table 6* on page 207.
WPA-PSK & WPA2-PSK **Note:** Use this option if there are both WPA-PSK and WPA2-PSK clients in the network.	TKIP + AES	To configure WPA-PSK & WPA2-PSK authentication: 1. (Optional) Select the **Show Passphrase** check box to display the characters in the WPA Passphrase (Network Key) field. 2. Type a passphrase of at least eight characters in the WPA Passphrase (Network Key) field. **Note:** The Data Encryption menu displays TKIP + AES, which is the only available option. Both TKIP and AES are supported. **Note:** For information about requirements for a WPA passphrase, see *Table 6* on page 207.

Manage MAC Authentication and MAC Authentication Groups

MAC authentication lets you set up an external or a local access control list (ACL) with MAC addresses of clients to either allow or deny the network access privilege of the specified clients with the wireless controller–managed access point. The settings are applied only to managed access points.

Note: The wireless controller can support an aggregate number of 4096 MAC addresses for all its local ACLs.

Guidelines for External MAC Authentication

Note the following external RADIUS server guidelines:

- For each MAC authentication client, you need to configure a policy on the RADIUS server.
- During MAC authentication, the wireless controller sends the following information to the RADIUS server:
  - MAC address in the format xx:xx:xx:xx:xx:xx
  - User name
  - Calling station ID
- The wireless controller uses CHAP as the authentication protocol with the RADIUS server.
- You can configure either MAC authentication with an external RADIUS server or network authentication with an external RADIUS server, but not both. That is, if you configure an external RADIUS server with WPA, WPA2, or WPA & WPA2, you cannot use external MAC authentication but are limited to internal MAC authentication.

➢ **To use an external ACL:**

1. Configure an ACL on an external RADIUS server.
2. On an Edit Profile screen for the basic profile group or an advanced profile group, next to MAC ACL, select the **External** radio button.
3. From the External Radius Server menu, select the external authentication server.

   For more information, see *Configure Security Profiles for the Basic Profile Group* on page 67 and *Configure Security Profiles for Advanced Profile Groups* on page 71.

The wireless controller consults the MAC ACL at initial client authentication. While a client roams, the wireless controller uses cached authentication information. After a client has disassociated from the access point and then attempts to reassociate, the wireless controller once again consults the MAC ACL.

Configure Basic Local MAC Authentication Settings

You would typically use the basic MAC authentication group in the profiles of a basic profile group of a small-scale network. However, you can assign the basic MAC authentication group to *any* profile, whether in the basic profile group or in an advanced profile group.

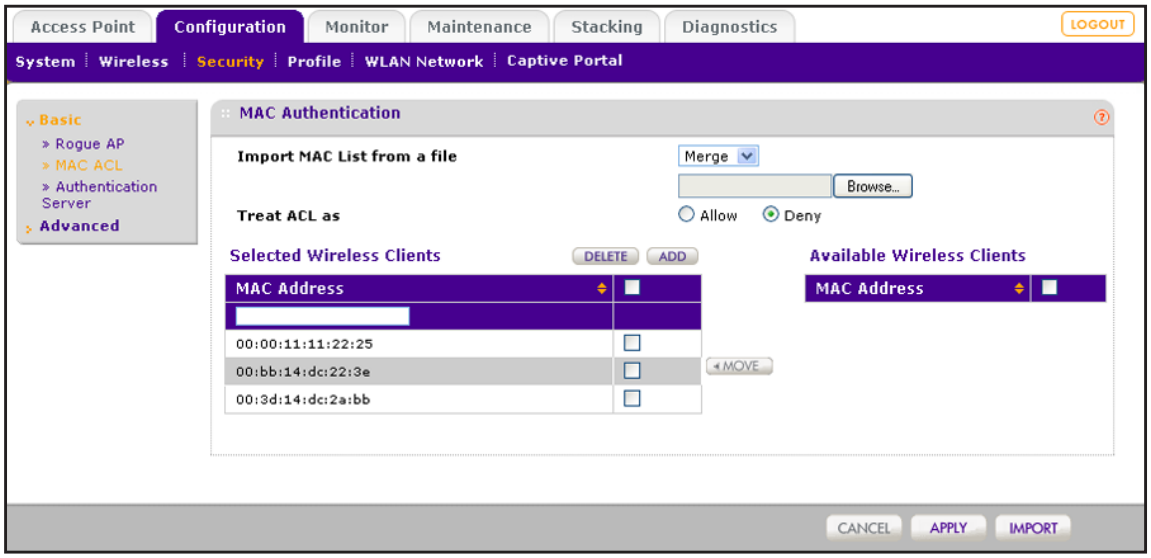
The wireless controller supports a maximum of 256 MAC addresses per SSID.

Note: You cannot add multicast or broadcast MAC addresses to a MAC access control list (ACL).

➢ **To set up basic MAC authentication ACL:**

1. Select **Configuration > Security > Basic > MAC ACL**.

   The basic MAC Authentication screen displays:



   Note: *As an option, you can import a list of MAC addresses from a file. For more information, see the next section.*

2. Next to Trust ACL as, select one of the following radio buttons:
   - **Allow**. Network access is granted to the clients for which the MAC addresses are listed in the Selected Wireless Clients list.
   - **Deny**. Network access is denied to the clients for which the MAC addresses are listed in the Selected Wireless Clients list.

3. Add wireless clients to the Selected Wireless Clients list through one of the following methods:
   - The MAC address that you want to add is in Available Wireless Clients list, which contains wireless stations that are present in the vicinity of the access point:
     a. Select the MAC address from the Available Wireless Clients list.
     b. Click **Move**.
   - The MAC address that you want to add is not in Available Wireless Clients list:
     a. Enter the MAC address in the MAC Address field.
     b. Click **Add**.
4. Click **Apply**.

➢ **To remove a MAC address from the Selected Wireless Clients list:**

1. Select the check boxes that correspond to the MAC addresses that you want to remove.
2. Click **Delete**.
3. Click **Apply**.

For information about how to add a MAC ACL to a security profile in the basic profile group, see *Configure Profiles in the Basic Profile Group* on page 67.

For information about how to add a MAC ACL to a security profile in an advanced profile group, see *Configure Profiles in an Advanced Profile Group* on page 73.

Import a MAC List from a File

You can import a precompiled list of MAC addresses from a saved file. This file needs to be a simple text file with one MAC address per line.

➢ **To import a MAC list from a file:**

1. Create a text file that includes a list of MAC addresses.

   Each MAC address should be on a separate line with hard returns between lines as shown in the following example:

```
00:00:11:11:22:29
00:00:11:11:22:28
00:00:11:11:22:27
00:00:11:11:22:26
00:00:11:11:22:25
```

2. Select **Configuration > Security > Basic > MAC ACL**.

   The basic MAC Authentication screen displays.

3. Click **Browse**, navigate to the file containing the list of MAC addresses, and select it.
4. Make one of the following selections from the Import MAC List from a file menu:
   - **Merge**. Merges the list of MAC addresses that you intend to import with those that are already present in the Selected Wireless Clients list.
   - **Replace**. Replaces the MAC addresses that are present in the Selected Wireless Clients list with those in the file that you intend to import.

5. Click **Import**.
6. Click **Apply**.

Configure Local MAC Authentication Groups

For greater security flexibility, you can create up to eight MAC authentication groups (MAC ACLs) to block or allow network access privilege of different clients. You can assign any MAC authentication group, including the basic MAC authentication group, to *any* profile, whether in the basic profile group or in an advanced profile group.

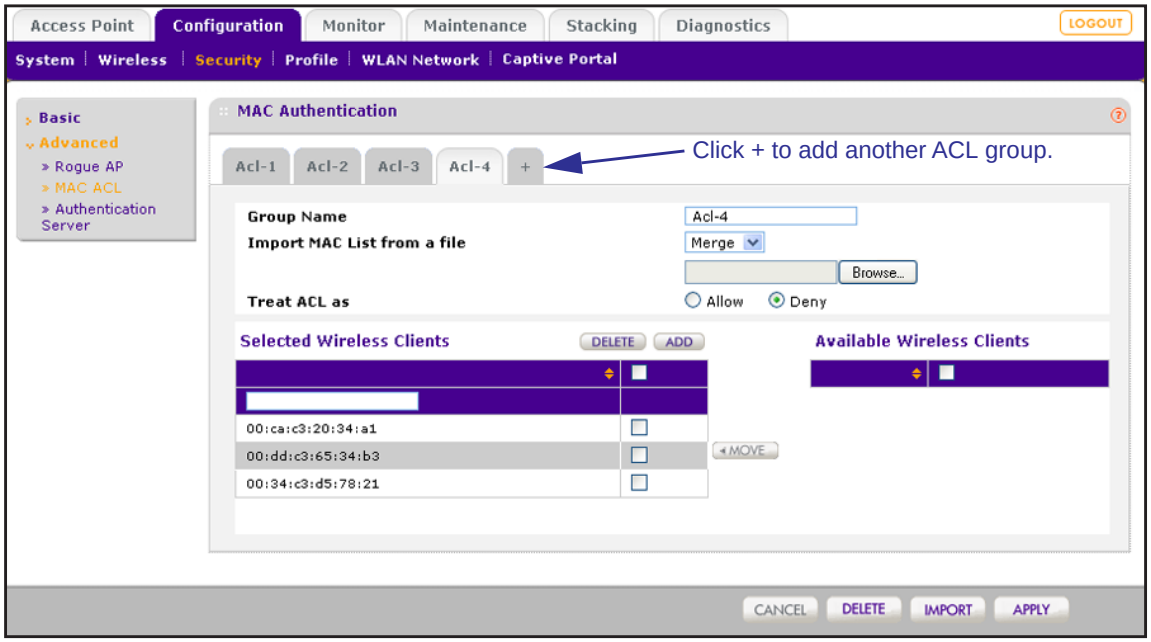
The wireless controller supports a maximum of 256 MAC addresses per SSID.

Note: You cannot add multicast or broadcast MAC addresses to a MAC access control list (ACL).

➢ **To set up a MAC authentication group:**

1. Select **Configuration > Security > Advanced > MAC ACL**.

   The advanced MAC Authentication screen displays:



2. Click the **+** button to create an additional ACL group.
3. The new ACL group displays on the advanced MAC Authentication screen, and the tab for the new ACL is automatically selected to let you configure the new group.
4. (Optional) In the Group Name field, enter a unique name for the ACL group.

   By default, profile groups are named Acl-1, Acl-2, Acl-3, and so on.

5. Compile the Selected Wireless Clients list.

   For information about how to compile a wireless clients list, see *Configure Basic Local MAC Authentication Settings* on page 82.

6. Click **Apply**.

For information about how to add a MAC authentication group to a security profile in the basic profile group, see *Configure Profiles in the Basic Profile Group* on page 67.

For information about how to add a MAC authentication group to a security profile in an advanced profile group, see *Configure Profiles in an Advanced Profile Group* on page 73.

➢ **To delete an ACL group:**

1. Select **Configuration > Security > Advanced > MAC Authentication**.

   The advanced MAC Authentication screen displays:

2. Click the tab for the ACL group that you want to delete.
3. Click **Delete**.

Manage Authentication Servers and Authentication Server Groups

You can specify three types of authentication servers: internal, external RADIUS, and external LDAP:

- **Internal authentication server**. The wireless controller handles authentication. If you use this setting, set up WiFi clients on the User Management screen (see *Manage Users, Accounts, and Passwords* on page 116.)
- **External RADIUS server**. You can define a basic external RADIUS server that you would typically use in the profiles of a basic profile group of a small-scale network. You need to specify its configuration on the basic Authentication Server screen (see the next section) so that you can select this authentication option during the configuration of a profile. As part of the advanced authentication server settings, you can define multiple external RADIUS servers that you would typically use in a more complex network with many profiles. You can then assign different RADIUS servers to different profiles.

  By default, the external RADIUS server for the basic authentication group is called basic-Auth. You cannot change this name. By default, the external RADIUS authentication servers for the advanced authentication groups are called Auth1 through Auth8, and you *can* change these names. You can assign the basic-Auth server to an advanced profile group, and you can assign a RADIUS server of an advanced authentication group to the basic profile group.

See the following configuration guidelines for external RADIUS servers:

- You need to add only the IP address of the wireless controller as a RADIUS client to the RADIUS server. All managed access points are then automatically known to the RADIUS server.
- For configuration guidelines for external MAC authentication, see *Guidelines for External MAC Authentication* on page 81.
- For configuration guidelines for external authentication of captive portal users, see *Manage Guest Network Access* on page 111.

- **External LDAP server**. You can define one external LDAP server (commonly referred to as an Active Directory [AD] server). You need to specify its configuration on the basic Authentication Server screen (see the next section) so that you can select this authentication option during the configuration of a profile.

  By default, the external LDAP server for the basic authentication group is called basic-LDAP. You cannot change this name, and you cannot configure any LDAP servers for the advanced authentication groups. You can assign the basic-LDAP server to both the basic profile group and to advanced profile groups.

All three servers can be active so that the profiles that you set up can be configured to work with different authentication servers. For example, you could set up a guest profile with no authentication, an engineering profile that uses external RADIUS authentication, and a marketing profile that uses external LDAP authentication.

The settings that you specify on the Authentication Server screen affect the selections that are available in the Network Authentication menu and the corresponding Authentication Server field on the Edit Profile screens. For information about how to configure security profiles, see *Configure Profiles in the Basic Profile Group* on page 67 and *Configure Profiles in an Advanced Profile Group* on page 73.

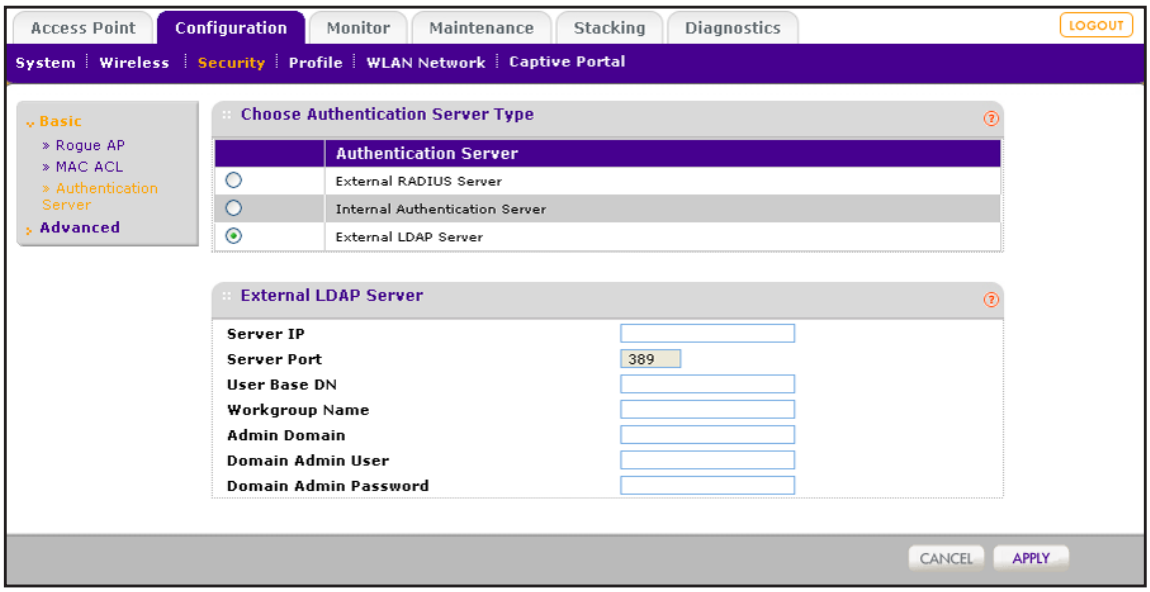
Configure Basic Authentication Server Settings

Use the basic Authentication Server screen to set up the internal authentication server, the basic external RADIUS server (which is called Auth-basic), and the external LDAP server (which is called Auth-LDAP). After you have set up these authentication servers, you can assign any of them to *any* profile, whether in the basic profile group or in an advanced profile group.

➢ **To configure a basic authentication server:**

1. Select **Configuration > Security > Basic > Authentication Server**.

The basic Authentication Server screen displays. The following figure shows the fields for an external LDAP server:



2. Select the radio button that corresponds to the authentication server that you want to set up:
   - **External RADIUS Server**
   - **Internal Authentication Server**
   - **External LDAP Server**
3. Configure the settings that correspond to the selected authentication server as described in the following table:

Setting	Description		
External RADIUS Server	Enable Authentication	Select this check box to enable authentication.	
	Enable Accounting	Select this check box to enable accounting.	
	Primary Server	Do the following for each server: 1. Specify the IP address. 2. Specify the port. The default port is 1812. 3. Specify the shared secret.	For information about shared secret requirements, see *Table 6* on page 207.
	Secondary Server		
	Reauthentication time (Seconds)	Specify the time (in seconds) after which reauthentication occurs for all wireless clients.	
	Update Global Key Every (Seconds)	To enable update of the global key: 1. Select this check box. 2. Specify the interval (in seconds) after which the global key is updated for all wireless clients.	

Setting	Description		
Internal Authentication Server	Reauthentication Time (seconds)	Specify the time (in seconds) after which reauthentication occurs for all wireless clients.	When you use the internal authentication server, set up WiFi clients on the User Management screen. For information, see *Manage Users, Accounts, and Passwords* on page 116.
	Update Global Key Every (seconds)	To enable update of the global key: 1. Select this check box. 2. Specify the interval (in seconds) after which the global key is updated for all wireless clients.	
External LDAP Server	Server IP	Specify the IP address of the external Active Directory (AD) authentication server.	
	Server Port	Specify the port of the external AD server. The default is port 389.	
	User Base DN	Specify the user base distinguished name (DN) on the AD server.	
	Workgroup Name	Specify the workgroup name on the AD server.	
	Admin Domain	Specify the administrative domain on the AD server.	
	Domain Admin User	Specify the user name for the administrative domain.	
	Domain Admin Password	Specify the password for the administrative domain. **Note:** For information about password requirements, see *Table 6* on page 207.	

4. Click **Apply**.

For information about how to add an authentication server to a security profile in the basic profile group, see *Configure Profiles in the Basic Profile Group* on page 67.

For information about how to add an authentication server to a security profile in an advanced profile group, see *Configure Profiles in an Advanced Profile Group* on page 73.

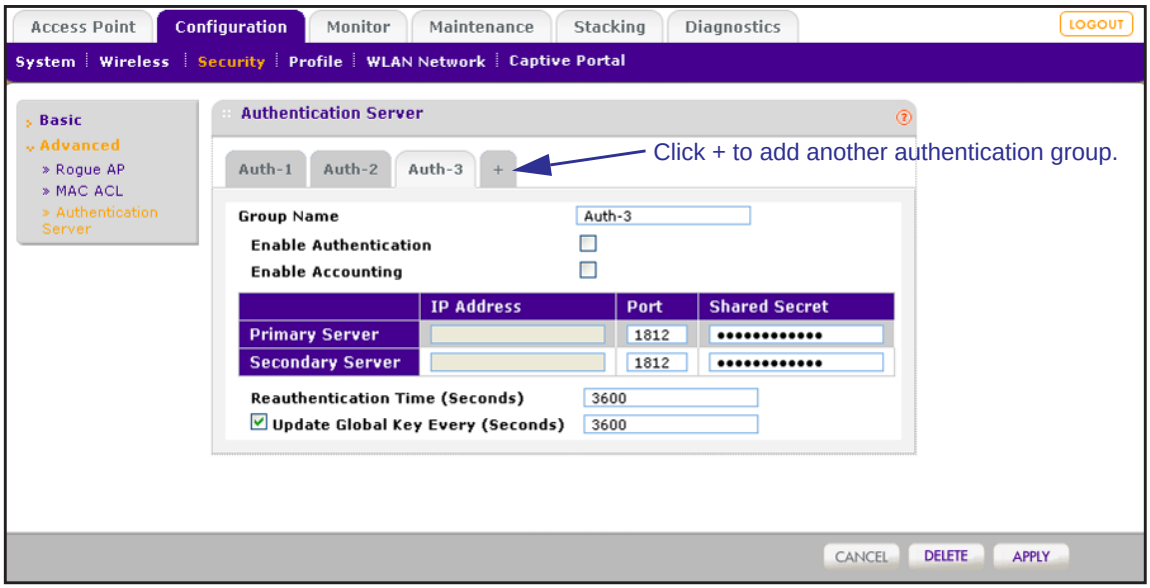
Configure RADIUS Authentication Server Groups

For greater security flexibility, you can create up to eight external RADIUS servers to authenticate different groups of users. After you have set up these authentication servers, you can assign any of them, including the basic RADIUS server, to *any* profile, whether in the basic profile group or in an advanced profile group.

➢ **To set up a RADIUS authentication server group:**

1. Select **Configuration > Security > Advanced > Authentication Server**.

The advanced Authentication Server screen displays:



2. Click the **+** button to create an additional authentication group.

   The new authentication group displays on the advanced Authentication Server screen, and the tab for the new authentication is automatically selected to let you configure the new group.

3. (Optional) In the Group Name field, enter a unique name for the authentication group.

   By default, authentication groups are named Auth-1, Auth-2, Auth-3, and so on.

4. Configure the external RADIUS server for the group.

   For information about setting up an external RADIUS server, see the table in the previous section, *Configure Basic Authentication Server Settings* on page 86.

5. Click **Apply**.

For information about how to add a RADIUS authentication group to a security profile in the basic profile group, see *Configure Profiles in the Basic Profile Group* on page 67.

For information about how to add a RADIUS authentication group to a security profile in an advanced profile group, see *Configure Profiles in an Advanced Profile Group* on page 73.

➢ **To delete a RADIUS authentication group:**

1. **Configuration > Security > Advanced > Authentication Server**.

   The advanced Authentication Server screen displays.

2. Click the tab for the RADIUS authentication group that you want to delete.
3. Click **Delete**.

Discover and Manage Access Points

6

This chapter includes the following sections:

- *Access Point Discovery Guidelines*
- *Discover Access Points with the Discovery Wizard*
- *Manage the Managed AP List*
- *Assign Access Points to Advanced Profile Groups*

IMPORTANT:

Before you use the wireless controller to discover your access points and push the configurations to the access points:

1. Make sure that you have registered sufficient licenses.

2. Determine which profiles and security you require.

3. If needed, set up authentication servers and MAC authentication.

4. Complete the configuration of the profiles that you intend to use.

These steps are described in *Register Your Licenses* on page 54 and in *Chapter 5, Manage Security Profiles and Profile Groups*.

Access Point Discovery Guidelines

You need to run the Discovery Wizard for the wireless controller to discover supported NETGEAR access points on the LAN or WAN. The wireless controller can discover access points that are still in their factory default state and access points that are deployed and running.

After the access points are discovered, you can add them to the Managed AP List. You can then use the wireless controller to configure, manage, and monitor the managed access points.

General Discovery Guidelines

An access point needs to run at least its initial firmware release or a newer version. For firmware requirements, see *NETGEAR ProSAFE Access Points* on page 15. There are no other firmware requirements for the access point to function with the wireless controller.

Access points in factory default state that are in the same Layer 2 network can have the same IP address and still be discovered. Depending on the configuration of the DHCP server, these access points are discovered in parallel or sequentially.

Layer 3 Discovery Guidelines

These are the requirements for autodiscovery of local access points across Layer 3 networks:

- All standalone access points need to have SNMP and SSH enabled. (This is the default setting for access points.)
- UDP port number 7890 needs to be unblocked in the firewall.
- Each access point needs to have a unique IP address. (This requirement does not apply to Layer 2 discovery.) If more than one access point has the same IP address, only one of them is discovered at a time. You have to add the access point to the managed list, change its IP address, and run discovery again to discover the next access point with that IP address.
- DHCP option 43 (vendor-specific information) needs to be enabled on an *external* DHCP server. Specifying an internal DHCP server on the wireless controller automatically enables DHCP option 43 with the IP address of the wireless controller.

  How you need to configure DHCP option 43 depends on the type of external DHCP server:

  - **Layer 3 switch as a DHCP server**. If you use a Layer 3 switch as a DHCP server, specify the wireless controller's IP address in hexadecimal format to allow the access points to receive the wireless controller's IP address and to allow the DHCP server to assign IP addresses to the access points. The hexadecimal address needs to be preceded by the vendor-specific octets 02:04:.

To compose the address, start with 02:04: and then add each of the four address octets in hexadecimal format, separated by colons. For example:

192.168.33.27 in decimal format equals c0:a8:21:1b in hexadecimal format. After you have added the vendor-specific octets, the complete address is 02:04:c0:a8:21:1b.

- **Linux- or Windows-based DHCP server**. If you use a Linux- or Windows-based DHCP server, configure the IP address in decimal format and NETGEAR_WNC_AP as the vendor class identifier.

Discover Access Points with the Discovery Wizard

The Discovery Wizard finds provides two methods to find access points that are not yet on the managed access point list. These methods are described in the following sections:

- *Access Points in Factory Default State and Access Points in a Layer 2 Subnet*
- *Access Points Installed and Working in Standalone Mode in Different Layer 3 Networks*

CAUTION:

If security is not set up, or is set up incorrectly, when the wireless controller pushes the configurations to the access points, you could accidentally wipe out all security, leaving your entire network open to access. Be sure that you set up security correctly (see *Chapter 5, Manage Security Profiles and Profile Groups*).

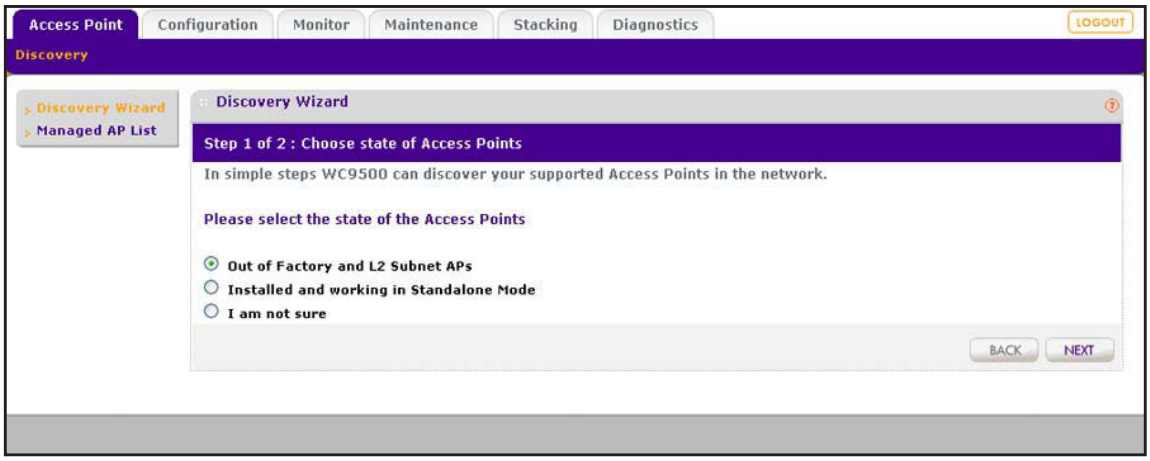
Access Points in Factory Default State and Access Points in a Layer 2 Subnet

Access points in factory default state are access points “out of the box” that have never been employed. Access points in a Layer 2 subnet are access points that are installed and functioning in the same IP subnet as the wireless controller and that are connected to the wireless controller through a back-end Layer 2 switch.

➢ **To discover access points in factory default state and access points in a Layer 2 subnet:**

1. Select **Access Point > Discovery Wizard**.

The Discovery Wizard Step 1 of 2 : Choose state of Access Points screen displays:

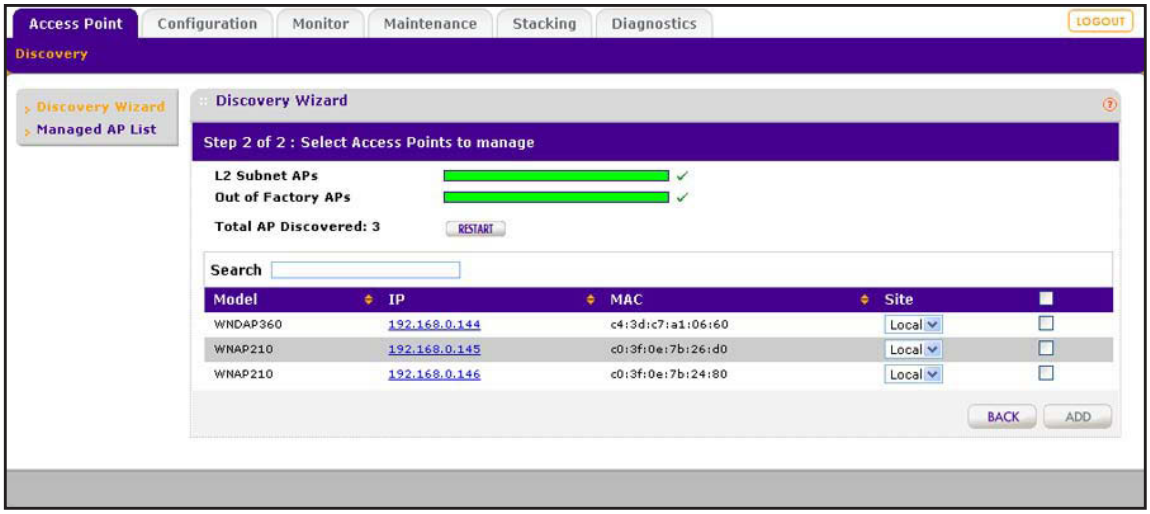


2. Select the **Out of Factory and L2 Subnet APs** radio button.

   Note: *The I am not sure radio button directs you to the product documentation.*

3. Click **Next**.

   The Discovery Wizard Step 2 of 2 : Select Access Points to manage screen displays.



   The wireless controller searches for NETGEAR products on the LAN based on MAC address and identifies which products are supported access point models. Progress bars show the progress of the discovery process.

   When the discovery process is finished, the total number of access points is displayed and the table shows the access points that were discovered. For each access point, the table includes the model number, IP address, MAC address, and site.

4. (Optional) Enter information in the Search field to find an individual access point.
5. Review the discovery results to make sure that all the access points are listed.

The effectiveness of the discovery process depends in part on how the access points on your LAN are set up. If each access point is configured with a unique IP address and is running current firmware, discovery is usually simple.

If the discovery results are not what you expect, check the following:

- Access points that are already managed by the wireless controller are not in the discovery list.

  To view the Managed AP List, select **Access Point > Managed AP List**.

- The access points might be in a different IP network.

  For information about how to discover access points in a different subnet, see *Access Points Installed and Working in Standalone Mode in Different Layer 3 Networks* on page 96.

- Access points that are in factory default mode but across a router are not detected.

  For information about how to discover access points across a router, see *Access Points Installed and Working in Standalone Mode in Different Layer 3 Networks* on page 96.

- Make sure that a DHCP server is available in the network or on the wireless controller.

  For information about the wireless controller's DHCP server, see *Manage the DHCP Server* on page 51.

- For more information, see *Problems with Access Points* on page 202.

6. (Optional) Click **Restart**.

   The discovery process runs again.

7. (Optional) From the Site menu, select **Remote** for each access point that you want to designate as a remote access point.

   By default, all discovered access points are designated as Local. The Remote and Local designations are for organization only.

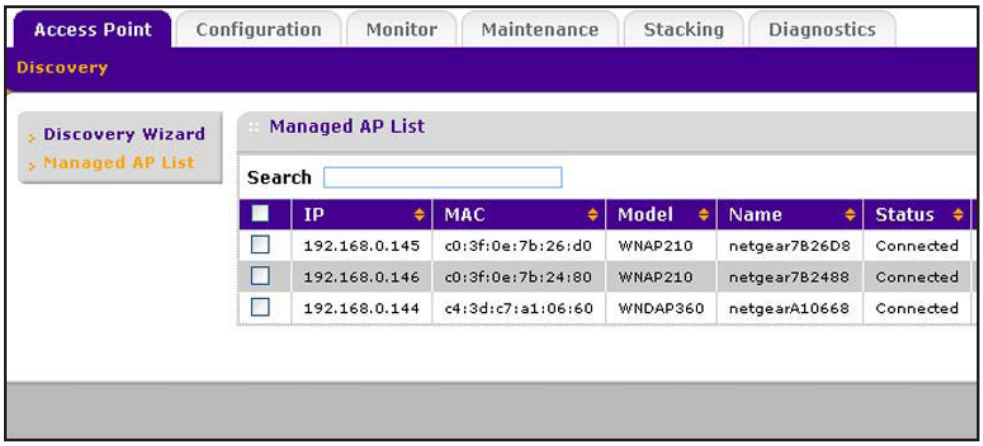
   Note: *The wireless controller cannot discover remote access points over a site-to-site VPN connection or behind a remote NAT router without a VPN connection. This capability will be added in a future release.*

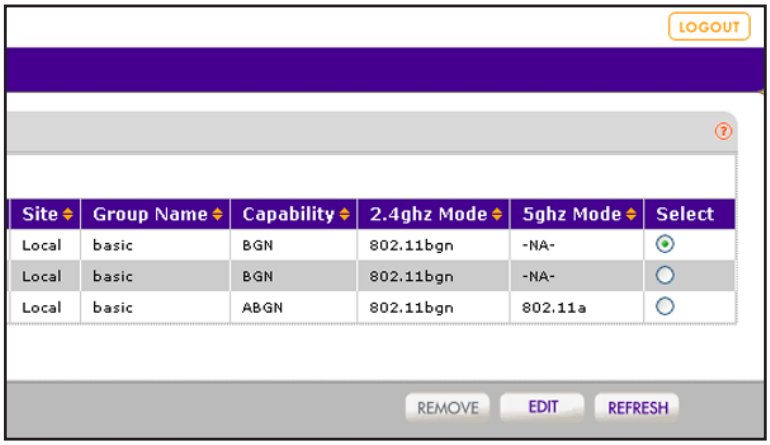
8. Do one of the following:
   - Select individual check boxes for discovered access points that you want to add to the managed list.
   - Select the check box in the upper right of the table heading to add all discovered access points to the managed list.
9. Click **Add**.

   Depending on the type of access points that have been discovered, a screen that lets you enter or ignore a login name and password might display.

10. If necessary, enter the login name and password.

    The Managed AP List screen displays. Because this is a wide screen, it is shown in the following two figures:





After the access points are added to the Managed AP List, the wireless controller upgrades the firmware of the access points to the latest firmware that is loaded on the wireless controller, and the access points become managed access points. Depending on the number of access points that you add to the Managed AP List, this process might take several minutes.

By default, the access point upgrade process uses multicast. If you need to configure a specific multicast IP address range for the upgrade process or disable multicast, see *Configure Multicast Firmware Upgrade for Access Points* on page 168.

If one or more access points do not transition to the Connected state (see the Status column in the Managed AP List), see *Problems with Access Points* on page 202.

For information about how to manage the Managed AP List, see *Manage the Managed AP List* on page 100.

Access Points Installed and Working in Standalone Mode in Different Layer 3 Networks

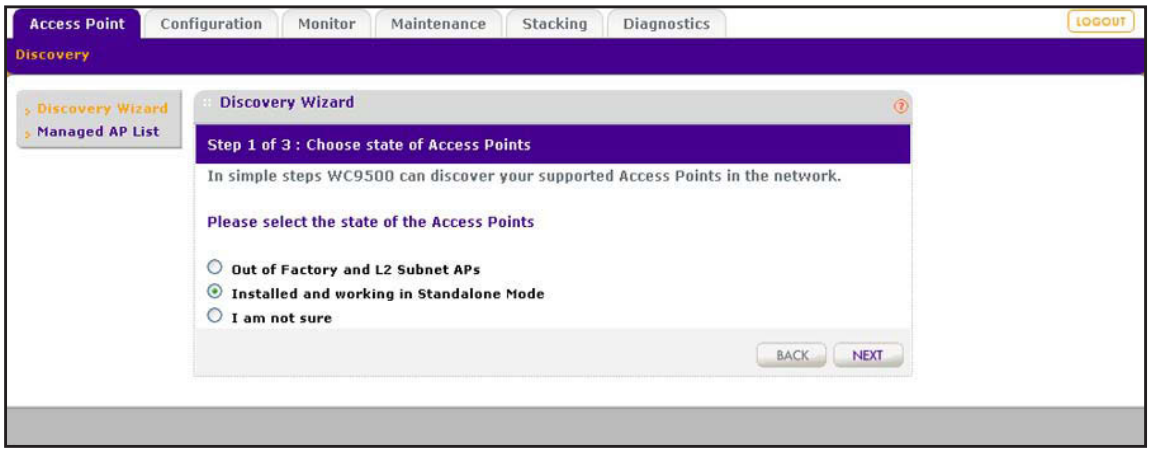
Access points that are installed and working in standalone mode in different Layer 3 networks are access points that do not function in the same subnet as the wireless controller but in different IP ranges and that are connected to the wireless controller through a router.

If you have a very large wireless network, you might have to run the Discovery Wizard several times.

➢ **To discover access points in different Layer 3 networks:**

1. Select **Access Point > Discovery Wizard**.

   The Discovery Wizard Step 1 of 3 : Choose state of Access Points screen displays:

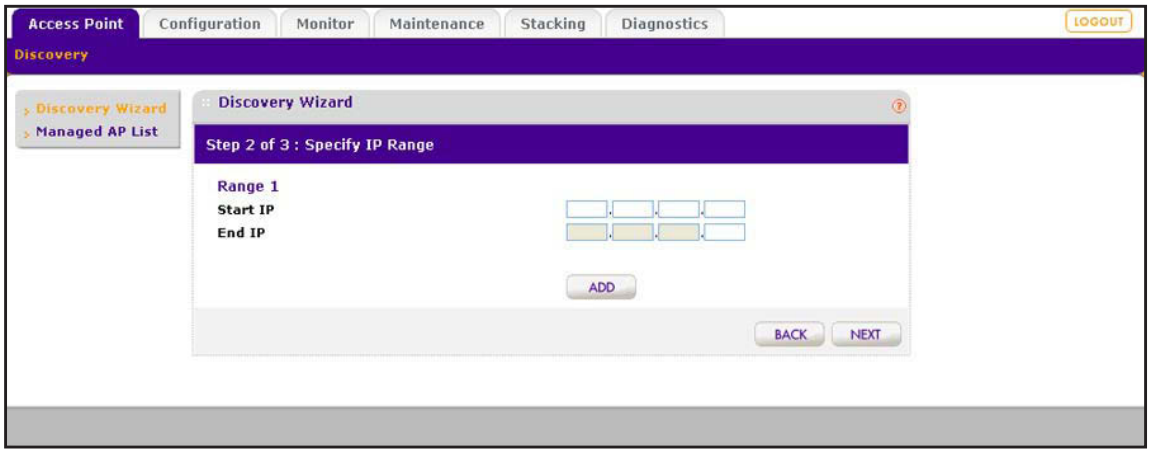


2. Select the **Installed and working in Standalone Mode** radio button.

   Note: *The I am not sure radio button directs you to the product documentation.*

3. Click **Next**.

   The Discovery Wizard Step 2 of 3 : Specify IP Range screen displays:



4. In the Range 1 section, fill in the Start IP and End IP fields.

   These IP addresses specify the range in which the wireless controller should discover access points.

5. (Optional) Add additional IP address ranges for the wireless controller to search in:
   a. Click **Add**.

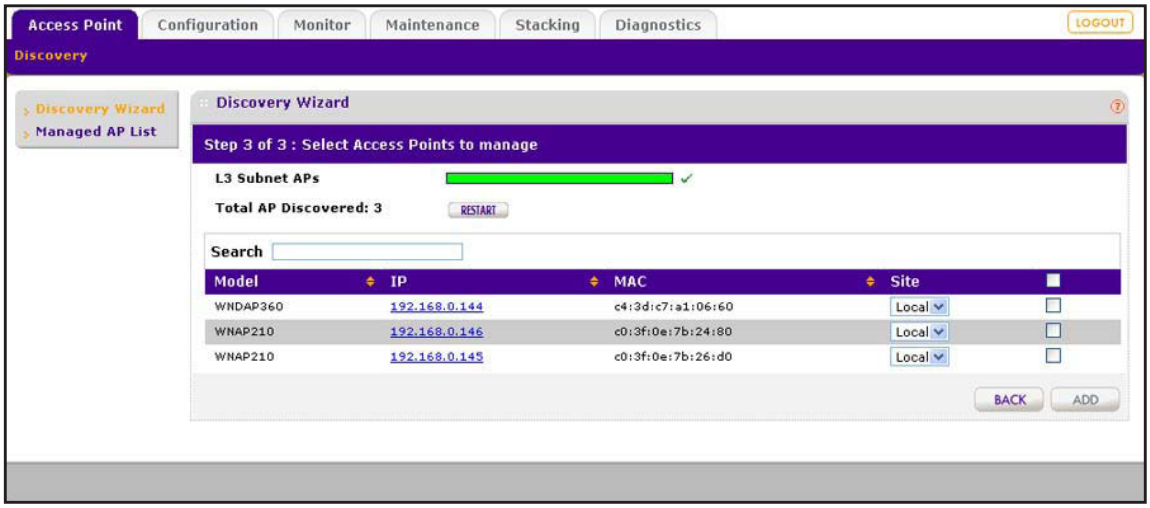
      The screen adjusts to display a second set of Start IP and End IP fields.

   b. In the Range 2 section, fill in the Start IP and End IP fields.
   c. Click **Add**.

      The screen adjusts to display a third set of Start IP and End IP fields.

   d. In the Range 3 section, fill in the Start IP and End IP fields.
6. Click **Next**.

   The Discovery Wizard Step 3 of 3 : Select Access Points to manage screen displays.



   The wireless controller searches for NETGEAR products on the LAN based on MAC address and then identifies which products are supported access point models. A progress bar show the progress of the discovery process.

   When the discovery process is finished, the total number of access points is displayed and the table shows the access points that were discovered. For each access point, the table includes the model number, IP address, MAC address, and site.

7. (Optional) Enter information in the Search field to find an individual access point.
8. Review the discovery results to make sure that all the access points are listed.

   The effectiveness of the discovery process depends in part on how the access points on your LAN are set up. If each access point is configured with a unique IP address and is running current firmware, discovery is usually simple.

If the discovery results are not what you expect, check the following:

- Access points managed already by the wireless controller are not in the discovery list.

  To view the Managed AP List, select **Access Point > Managed AP List**.

- Make sure that a DHCP server is available in the network or on the wireless controller.

  For information about the wireless controller's DHCP server, see *Manage the DHCP Server* on page 51.

- If more than one access point has the same IP address, only one of them is discovered at a time.

  You have to add the access point to the managed list, change its IP address, and run discovery again to discover the next access point with that IP address.

- For more information, see *Problems with Access Points* on page 202.

9. (Optional) Click **Restart**.

   The discovery process runs again.

10. (Optional) From the Site menu, select **Remote** for each access point that you want to designate as a remote access point.

    By default, all discovered access points are designated as Local. The Remote and Local designations are for organization only.

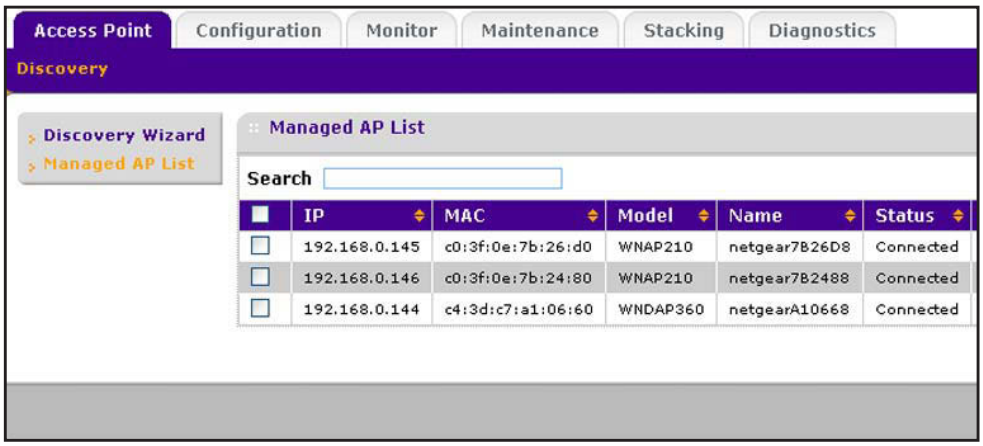
    Note: *The wireless controller cannot discover remote access points over a site-to-site VPN connection or behind a remote NAT router without a VPN connection. This capability will be added in a future release.*

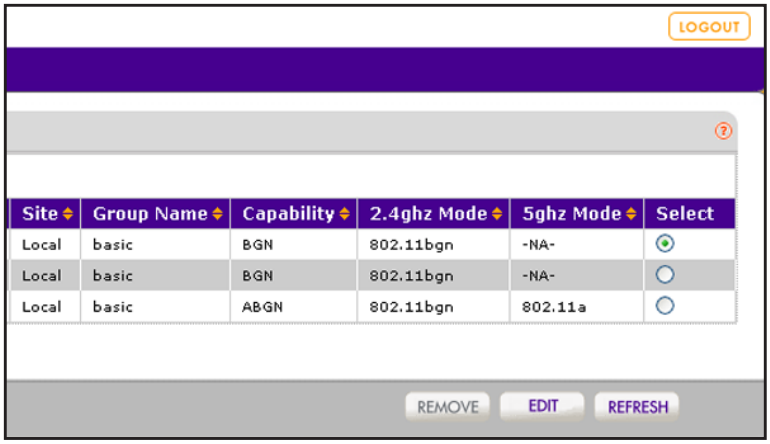
11. Do one of the following:
    - Select individual check boxes for discovered access points that you want to add to the managed list.
    - Select the check box in the upper right of the table heading to add all discovered access points to the managed list.
12. Click **Add**.

    Depending on the type of access points that have been discovered, a screen that lets you enter or ignore a login name and password might display.

13. If necessary, enter the login name and password.

The Managed AP List screen displays. Because this is a wide screen, it is shown in the following two figures:





After the access points are added to the Managed AP List, the wireless controller upgrades the firmware of the access points to the latest firmware that is loaded on the wireless controller, and the access points become managed access points. Depending on the number of access points that you add to the Managed AP List, this process might take several minutes.

By default, the access point upgrade process uses multicast. If you need to configure a specific multicast IP address range for the upgrade process or disable multicast, see *Configure Multicast Firmware Upgrade for Access Points* on page 168.

If one or more access points do not transition to the Connected state (see the Status column in the Managed AP List), see *Problems with Access Points* on page 202.

For information about how to manage the Managed AP List, see *Manage the Managed AP List* on page 100.

Manage the Managed AP List

After you have added discovered access points to the Managed AP List, you can view the status of the access points on the list, edit information for selected access point on the list, and remove access points from the list.

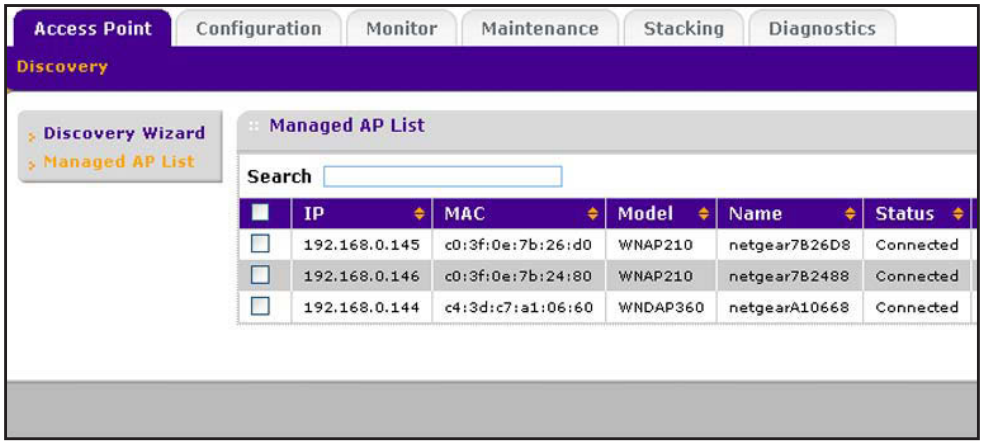
View the Managed AP List

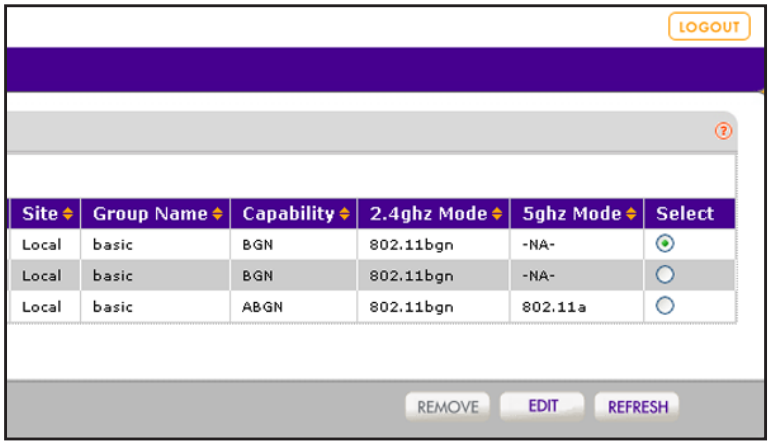
The managed AP List displays the status, IP addresses, MAC addresses, model numbers, names, and other information for the managed access points.

- **To view the status and other information for managed access points:**

  Select **Access Point > Managed AP List**.

  The Managed AP List screen displays. Because this is a wide screen, it is shown in the following two figures:





The Managed AP List screen shows the following entries for each access point that you added to the list:

Item	Description
IP	The IP address of the access point.
MAC	The MAC address of the access point.
Model	The model of the access point.
Name	The name of the access point.
Status	Shows one of the following status options: • **Authentication in progress**. This status can last several minutes. • **Applying configurations**. • **Firmware upgrade**. • **AP is rebooting**. • **Connecting**. Make sure that there is a DHCP server enabled in the network; otherwise, the managed access points remain in the Connecting state and do not enter the Connected state. • **Connected**. This status indicates normal operation. • **Not Connected**. The wireless controller cannot communicate with the access point at the configured IP address. The wireless controller tries to log in to managed access points each minute. If the error is temporary, the status automatically changes to Connected. If the error is prolonged, verify the access point's IP address and network connectivity. For more information, see *Problems with Access Points* on page 202.
Site	Shows whether you designated the access point as a local or remote one: • **Local**. The access point is designated as a local. • **Remote**. The access point is designated as remote.
Group Name	The default group is basic. For information about changing the group for an access point, see *Edit Access Point Information on the Managed AP List* on page 101.
Capability	The wireless modes that are supported by the access point. **Note:** Capability information lets you determine which access points are 802.11n mode capable but function in 802.11g mode.
2.4ghz Mode	The access point's wireless modes that function in the 2.4 GHz band.
5ghz Mode	The access point's wireless modes that function in the 5 GHz band.

Edit Access Point Information on the Managed AP List

For each individual access point, you can change the general information, IP settings, and VLAN settings, you can switch between the internal and external antenna (if the access point supports an external antenna), and you can enter location information.

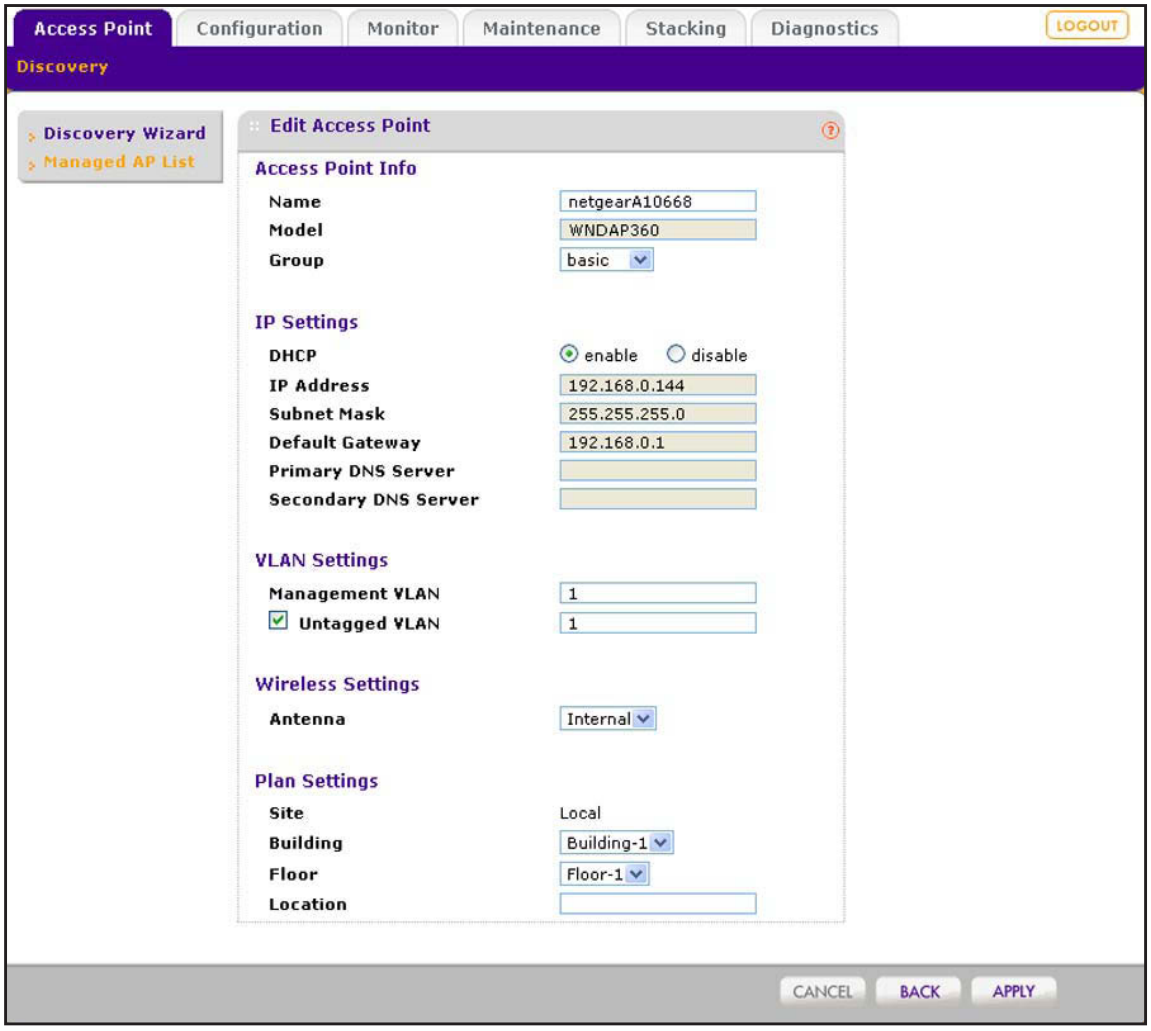
➢ **To edit the information for an access point on the Managed AP List:**

1. Select **Access Point > Managed AP List**.

   The Managed AP List screen displays.

2. Select the access point that you want to edit by selecting its radio button in the Edit column of the Managed AP List.
3. Click **Edit**.

   The Edit Access Point screen displays:



4. Configure the settings as described in the following table.

Setting	Description
Access Point Info section	
Name	Enter a unique value that indicates the access point name. By default, the name is netgearxxxxxx, where xxxxxx represents the last 6 hexadecimal digits of the access point's MAC address. You can change the name to one that is meaningful to you.
Model	The model of the access point. This field is populated during the access point discovery process and cannot be edited.

Setting	Description
Group	The group to which the access point is assigned. After the access point discovery process, the access point is automatically assigned to the basic group. If you have set up profile groups, you can assign the access point to another profile group by selecting one from the menu. You can also change the group assignment later on the WLAN Group Assignment screen. For more information, see *Assign Access Points to Advanced Profile Groups* on page 104.
IP Settings These fields show the IP address and other IP settings of the access point. By default, these fields are populated during the access point discovery process. These are the functions of the radio buttons: • **enable**. By default, the **enable** radio button is selected, allowing the access point to function as a DHCP client. The IP settings fields are masked out, preventing you from making changes. • **disable**. Select the **disable** radio button to disable the access point's DHCP client. The IP settings fields become available, allowing you to make changes, including changes to the access point's IP address.	
IP Address	The IP address of the access point.
Subnet Mask	The subnet mask of the access point.
Default Gateway	The default gateway of the access point.
Primary DNS Server	The primary DNS server of the access point.
Secondary DNS Server	The secondary DNS server of the access point.
VLAN Settings section	
Managed VLAN	Enter a VLAN ID or leave the default ID. By default, the management VLAN is 1. For more information about management VLANs, see *Management VLAN* on page 23 and *Management VLAN Concepts* on page 49.
Untagged VLAN	Enter a VLAN ID or leave the default ID. By default, the untagged VLAN is 1 and the Untagged VLAN check box is selected. When the wireless controller sends frames associated with the untagged VLAN to the LAN (Ethernet) interface, those frames are untagged. When the wireless controller receives untagged traffic from the LAN (Ethernet) interface, those frames are assigned to the untagged VLAN.
Wireless Settings section	
Antenna	You can specify which antenna the access point uses by making a selection from the menu: • **Internal**. The access point uses its internal antenna. • **External**. The access point uses its external antenna or antennas. External antennas are optional antennas that do not come standard with an access point.
Plan Settings section	
Site	The site designation is always Local.

Setting	Description
Building	The building designation is always Building-1, which is a fixed selection from the menu.
Floor	The floor designation is always Floor-1, which is a fixed selection from the menu.
Location	Enter a name that is meaningful to you.

5. Click **Apply**.
6. Click **Back**.

   The Managed AP List screen displays. Changes that you made on the Edit Access Point screen are displayed in the table.

7. (Optional) If the changes do not display in the table, click **Refresh**.

Remove Access Points from the Managed AP List

To restore a managed access point to its original firmware and use it once again as a standalone access point, remove the access point from the Managed AP List. Log in to the access point's web management interface, upgrade the firmware to the standalone AP firmware version, and reboot the access point.

➢ **To remove an access point from the Managed AP List:**

1. Select **Access Point > Managed AP List**.

   The Managed AP List screen displays.

2. Select the radio button to the right of the access point that you want to remove.
3. Click **Remove**.

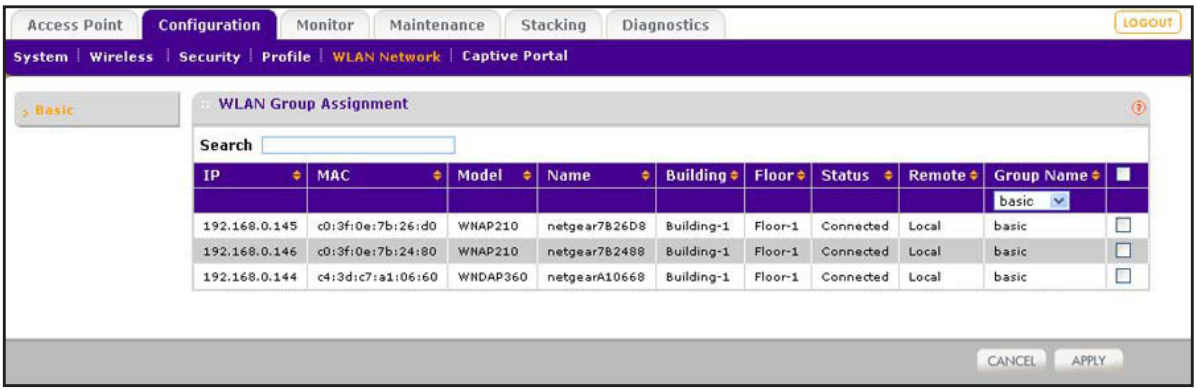
Assign Access Points to Advanced Profile Groups

By default, all access points are automatically assigned to the basic profile group. However, you can use the WLAN Group Assignment screen to assign access points to an advanced profile group. For information about how to create advanced profile groups, see *Advanced Profile Groups* on page 71.

Note: Access point profile group, profile group, and WLAN group are terms that are interchangeable.

➢ **To view the WLAN Group Assignment screen:**

Select **Configuration > WLAN Network**.



The settings are explained in the following table:

Setting	Description
IP	The IP address of the access point.
MAC	The MAC address of the access point.
Model	The model of the access point.
Name	The name that you specified for the access point.
Building	The building designation is always Building-1.
Floor	The floor designation is always Floor-1.
Status	• **Authentication in progress**. This status can last several minutes. • **Applying configurations**. • **Firmware upgrade**. • **AP is rebooting**. • **Connecting**. Make sure that there is a DHCP server enabled in the network; otherwise, the managed access points remain in the Connecting state and do not enter the Connected state. • **Connected**. This status indicates normal operation. • **Not Connected**. The wireless controller cannot communicate with the access point at the configured IP address. The wireless controller tries to log in to managed access points each minute. If the error is temporary, the status automatically changes to Connected. If the error is prolonged, verify the access point's IP address and network connectivity. For more information, see *Problems with Access Points* on page 202.
Remote	The site designation is always Local.
Group Name	The profile group to which the access point is assigned. For information about creating profile groups and their associated security profiles, see *Configure Security Profiles for Advanced Profile Groups* on page 71.

Tip: To view all members of a profile group, sort the access points by profile group. You do this by clicking the icon next to the Group Name header in the table.

➢ **To assign one or more access points to another profile group:**

1. Select **Configuration > WLAN Network**.

   The WLAN Group Assignment screen displays.

2. Take one of the following actions:
   - Assign a single access point to another group by selecting the check box to the right of the access point.
   - Assign a selection of access points to another group by selecting the check boxes to the right of the access points.
   - Assign all access points to another group by selecting the check box in the upper right of the table heading.
3. Select the group name from the Group Name menu in the table heading.
4. Click **Apply**.

7. Manage Rogue Access Points, Guest Network Access, and Users

This chapter includes the following sections:

- *Manage Rogue Access Points*
- *Manage Guest Network Access*
- *Manage Users, Accounts, and Passwords*

Manage Rogue Access Points

Rogue access point detection is disabled by default on the wireless controller. If you want to detect rogue access points, you need to enable rogue access point detection. Scanning might affect the service availability of the access point temporarily.

An access point is defined as rogue if:

- The access point's radio basic service set identifier (BSSID) is detected by any of the managed access points.
- The access point transmits on the Ethernet side on the same Layer 2 as the managed access points.
- At least one client is connected to the access point.

Any unmanaged access point not meeting all these conditions is classified as a neighbor.

The access points transmit broadcast frames on the Ethernet during the time access point radios are off-channel (and scanning).

The wireless controller can detect and maintain a maximum of 512 access points, both neighboring and rogue access points.

Note: If enabled, basic rogue AP detection and advanced rogue AP detection apply to all profiles, whether in the basic profile group or in any of the advanced profile groups.

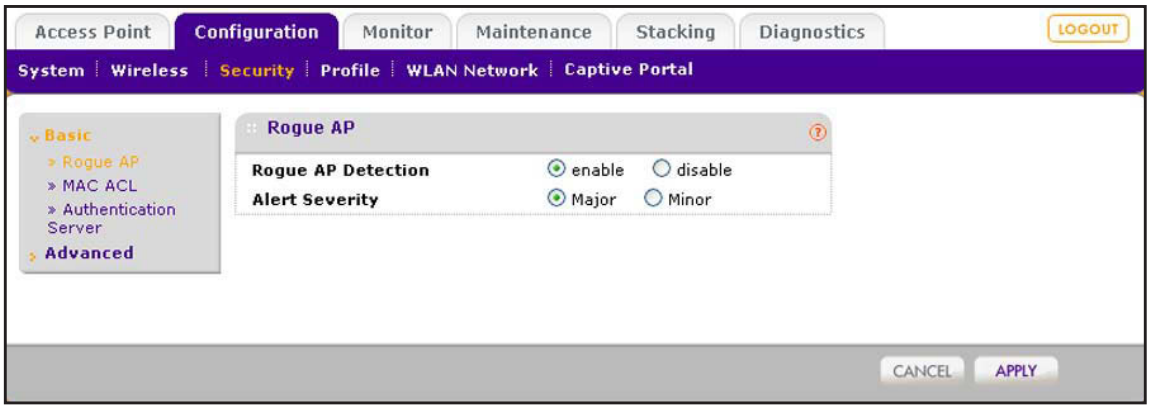
Configure Basic Rogue Detection Settings

In a basic setup, you can set up one detection server. In an advanced setup you can create multiple detection servers (for more information, see *Classify Rogue Access Points* on page 109).

➢ **To set up a server to detect rogue access points:**

1. Select **Configuration > Security > Basic > Rogue AP**.

The basic Rogue AP screen displays:



The wireless controller can support a total of up to 512 access points from the known and unknown lists combined.

2. Next to Rogue AP Detection, select the **enable** radio button.
3. Next to Alert Severity, select the severity of the alarm when a rogue access point is detected:
   - **Major**. A major alarm is triggered.
   - **Minor**. A minor alarm is triggered.
4. Click **Apply**.

   Because the neighboring and rogue access points are detected during off-channel scans, it typically takes about 30 minutes after the rogue AP detection is enabled for the neighbor and rogue access points to be detected on one channel.

   Once the neighbor and rogue access points are detected, the wireless controller populates the known list (that is, the database with known access points) and unknown list (that is, the database with unknown access points).

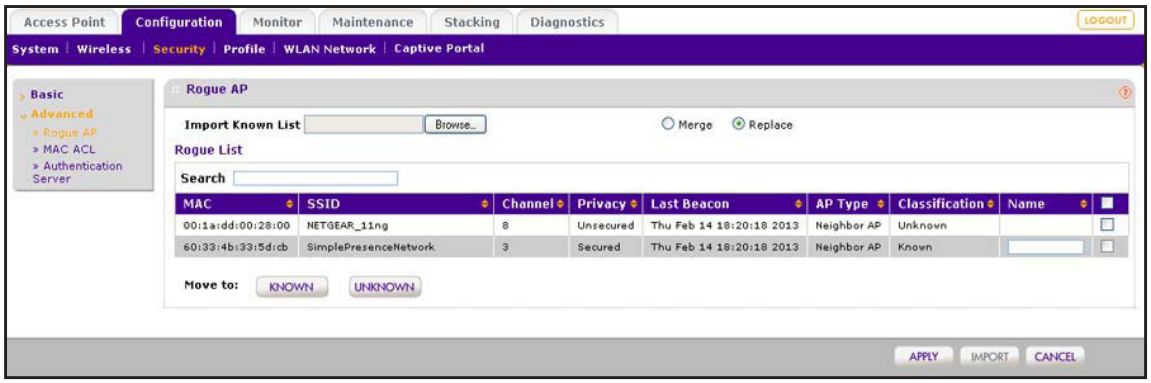
Classify Rogue Access Points

The advanced Rogue AP screen allows you to identify what could be an access point from a neighboring business that is known. As you identify them, mark them as known or unknown so that the wireless controller does not keep finding them and flagging them. This can help you to identify your own equipment that should be managed and the rogue access points that should be detected. A rogue access point has both a wireless and a LAN connection. A neighbor is an access point with only a wireless connection, not a LAN connection.

➢ **To view and classify rogue access points:**

1. Select **Configuration > Security > Advanced > Rogue AP**.

The advanced Rogue AP screen displays:



The screen displays the Rogue List, which shows all detected rogue access points with essential information, including information about their last beacon. If there are many entries that are spread out over several pages, click **Next** or **Previous** to scroll through the Rogue List.

Note: *As an option, you can import a list of access points from a file. For more information, see the next section.*

2. Classify the access points in the Rogue List:
   a. Do one of the following:
      - Select one or more check boxes that correspond to the access points.
      - Select all access points in the Rogue List by selecting the check box at the top of the table.
   b. Click one of the following two buttons, both of which are located below the Rogue List:
      - **Known**. Moves the selected access points to the known list.
      - **Unknown**. Moves the selected access points to the unknown list.
3. (Optional) For each known access point, enter a name in the Name column.

   This allows access points to be more easily identified.
4. Click **Apply**.

Import a List of Known Access Points from a File

You can import a list of known access points from a saved file. To do this, create a text file that includes the MAC address of each access point. This file needs to be a simple text file with one MAC address per line. The wireless controller can support a total of up to 512 access points from the known and unknown lists combined.

➢ **To import a list of known access points from a file:**

1. Create a text file that includes a list of MAC addresses for the access points. Each MAC address should be on a separate line with hard returns between lines as shown in the following example:

   ```
   00:00:11:11:22:29
   00:00:11:11:22:28
   00:00:11:11:22:27
   00:00:11:11:22:26
   00:00:11:11:22:25
   ```

2. Select **Configuration > Security > Advanced > Rogue AP**.

   The advanced Rogue AP screen displays.

3. Click **Browse**, navigate to the file containing the list of known access points, and select it.
4. Next to Import Known List, select one of the following radio buttons:
   - **Merge**. Merges the list of access points that you intend to import with those that are already present in the Rogue List.
   - **Replace**. Replaces the access points that are present in the Rogue List with those in the file that you intend to import.
5. Click **Import**.
6. Click **Apply**.

Manage Guest Network Access

Users with management (admin) credentials—for example, receptionists or hotel clerks—can provision guests. Guests need to provide their email address, or both their email address and a password. These latter guests are referred to as captive portal users, for which you need to set up a captive portal and captive portal user credentials.

Note: The URL for the portal is http://<*IP address*>/guest_access/index.php in which <*IP address*> is the IP address of the wireless controller.

Portal Concepts

Captive portal authentication is typically used for hotspot users and paying guests such as hotel guests who purchase access time for an Internet connection. You can configure only a single captive portal on the wireless controller.

When you configure a captive portal, you can use either the wireless controller as a local authentication server for the captive portal clients, or you can configure an external RADIUS server for authentication.

There are two types of portal settings:

- **Guest portal**. Use this portal if all wireless users are allowed to access the network by supplying only their email address. You do *not* need to define user names and passwords for these users.
- **Captive portal**. Use this portal type if wireless users need to supply their login name and password before being allowing access the network. You need to define user names and passwords for these users (see *Manage Users, Accounts, and Passwords* on page 116).

Note: You cannot configure captive portal authentication if the network authentication uses an external RADIUS server. That is, if you configure an external RADIUS server with WPA, WPA2, or WPA & WPA2 (or if you use legacy 802.1X), you cannot configure captive portal authentication; the network authentication needs to be Open System, Shared Key, WPA-PSK, WPA2-PSK, or WPA-PSK & WPA2-PSK (see *Network Authentication and Data Encryption Options* on page 77).

Note these guidelines for captive portal user authentication and accounting through an external RADIUS server:

- You can use either the basic-Auth RADIUS server or a RADIUS server of an advanced authentication group. You cannot use the external LDAP server.
- The wireless controller uses CHAP or MS-CHAP as the authentication protocol with the authentication server.
- The following RADIUS authentication variables are supported on the wireless controller:
  - User-Name
  - User-Password
  - WISPr-Session-Terminate-Time
  - Session-Timeout

  If you change the values for any of these variables before the wireless client disassociates from the access point, the new values are not updated on the wireless controller.
- A managed access point can send accounting information to the external RADIUS server because the wireless controller functions as a proxy RADIUS client for the managed access point. The following RADIUS accounting variables are supported on the wireless controller:
  - Acct-Input-Octets
  - Acct-Output-Octets
  - Acct-Input-Gigawords
  - Acct-Input-Gigawords

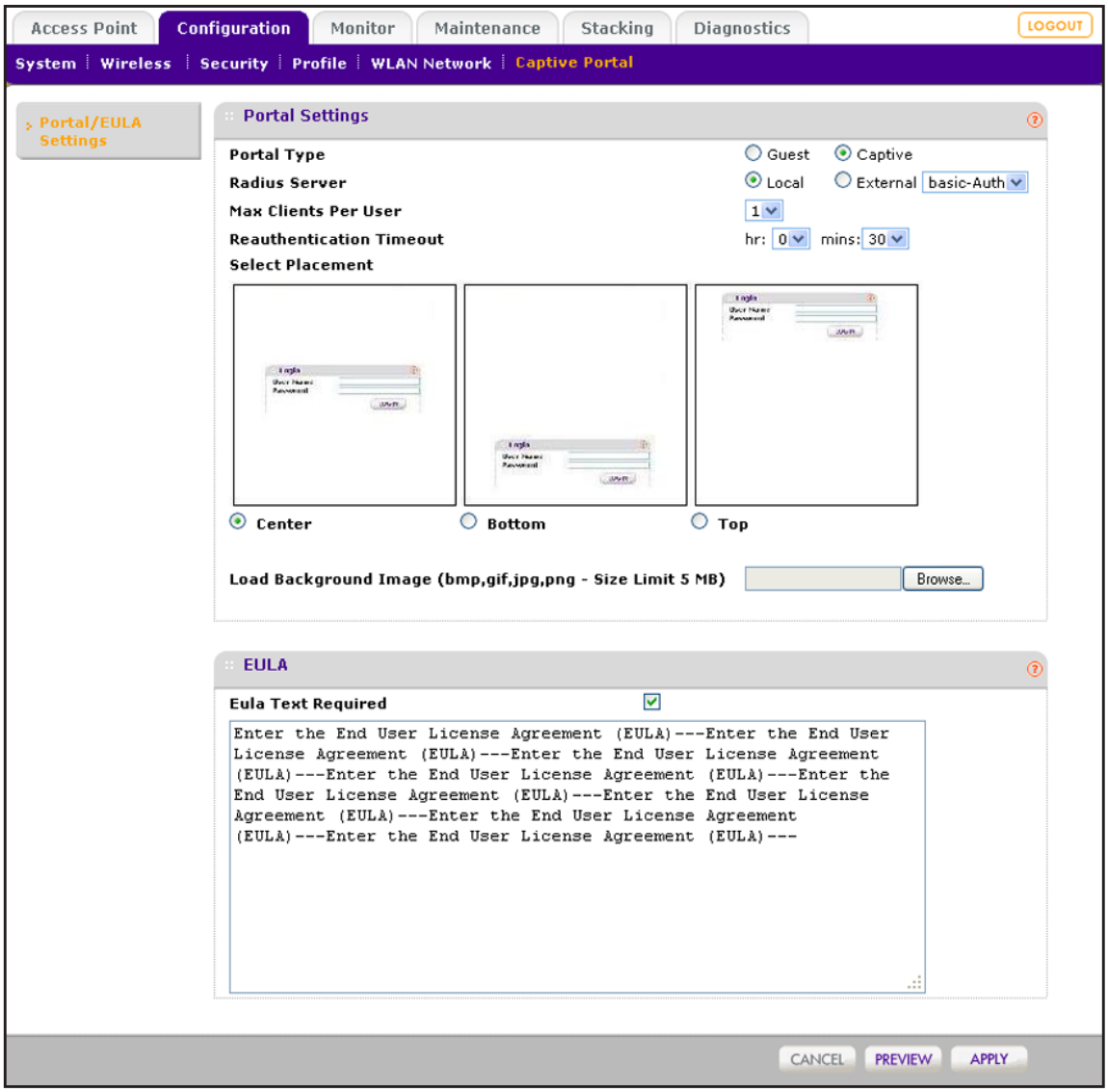
Configure a Portal

You can configure a guest portal or captive portal with a local or external authentication server.

➢ **To configure a guest portal or a captive portal:**

1. Select **Configuration > Captive Portal**.

   The Portal Settings screen displays. The following figure shows the settings for a captive portal. The settings for a guest portal are identical, except for the RADIUS server settings, which you cannot configure for a guest portal.



2. Configure the settings as described in the following table.

Setting	Description
Portal Settings section	
Portal Type	Select one of the following radio buttons: • **Guest**. A guest portal with a field for entering an email address. Guests do not need to provide a password and can have unlimited access to the network. You do not need to configure guest accounts. • **Captive**. A captive portal with a field for entering a login user name and a field for entering a password. If you select this option, the Radius Server radio buttons and menu display. For information about how to configure captive portal users and accounts, see *Manage Users, Accounts, and Passwords* on page 116.
Radius Server **Note:** This setting is for a captive portal only.	Select one of the following radio buttons: • **Local**. Use the local authentication server. • **External**. Select an external authentication server from the drop-down list. **Note:** For information about setting up and enabling internal and external authentication servers, see *Manage Authentication Servers and Authentication Server Groups* on page 85.
Max Clients Per User	Specify the number of clients that a single captive portal user can open with the same the login information. The default setting is 1. The maximum number of clients that you can select from the menu is 5.
Reauthentication Timeout	Specify the period after which a user who has been idle needs to be reauthenticated. The minimum period is 30 minutes. The maximum period that you can select is through the menus is three hours.
Select Placement	Select **Center**, **Bottom**, or **Top** to specify the location of the login prompt on the login screen.
Load Background Image	(Optional) Click **Browse** to navigate to and select an image file for the background of the login screen. You can use a .gif, .,jpg, or .bmp image.
EULA section	
EULA Text Required	Select this check box if you want to present the end user license agreement (EULA) on the guest login screen or captive portal login screen so users can view the EULA before they log in. Enter the EULA text in the text field.

3. (Optional) Click **Preview**.

   The portal settings that you have configured display. The default URL for the captive portal is http://192.168.0.250/guest_access/index.php.

4. Click **Apply**.

5. Assign the captive portal or guest portal to a security profile in the basic profile group, in an advanced profile group, or in both:
   - **Basic profile group**. Assign the captive portal or guest portal to a security profile in the basic profile group:
     a. Select **Configuration > Profile > Basic > Radio**.

        The Edit Profile (Basic) screen displays.

     b. Click the tab for the radio for which you want to assign the portal.
     c. Click the tab for the profile to which you want to assign the portal.
     d. In the Authentication Settings section of the screen, select the **Captive Portal** check box.

        The Captive Portal check box displays only when you select Open System, Shared Key, WPA-PSK, WPA2-PSK, or WPA-PSK & WPA2-PSK from the Network Authentication menu.

     e. Click **Apply**.
   - **Advanced profile group**. Assign the captive portal or guest portal to a security profile in an advanced profile group:
     a. Select **Configuration > Profile > Advanced > Radio**.

        The Profile Groups screen displays.

     b. Click the tab for the profile group for which you want to assign the portal.
     c. Click **Edit**.

        The Edit Profile screen displays.

     d. Click the tab for the radio for which you want to assign the portal.
     e. Click the tab for the profile to which you want to assign the portal.
     f. In the Authentication Settings section of the screen, select the **Captive Portal** check box.

        The Captive Portal check box displays only when you select Open System, Shared Key, WPA-PSK, WPA2-PSK, or WPA-PSK & WPA2-PSK from the Network Authentication menu.

     g. Click **Apply**.

Manage Users, Accounts, and Passwords

The wireless controller supports three types of users: management users, WiFi clients, and captive portal users. *All* of these users need to provide their login name and password to be authenticated by the wireless controller's internal authentication server and to access the wireless controller's web management interface or wireless network.

- **Management users**. These users have access to the wireless controller's web management interface. There are four groups:
  - **Administrators**. Administrative users (admins) with read and write capabilities. These users can change the configuration of the wireless controller.
  - **Read-only**. These users have access to the wireless controller's web management interface but can access only the Monitor main navigation tab and the Help main navigation tab. These users cannot change the configuration of the wireless controller.
  - **Guest provisioning**. These users can configure only captive portal users, that is, they can access only the User Management configuration menu tab under the Maintenance main navigation tab.
  - **License management only**. These users can configure only licenses, that is, they can access only the License configuration menu tab under the Maintenance main navigation tab (for more information, see *Manage Licenses* on page 165).
- **WiFi clients**. Users with credentials to access the wireless network. These users do not need to use the captive portal or the guest portal to access the wireless network, nor is their access subject to expiration.
- **Captive portal users**. Users with credentials to access the captive portal and who are granted temporary access or access without expiration.

In addition to the users, you can also configure captive portal accounts that you use in combination with captive portal users. Accounts specify the period during which wireless access is available and the amount that is charged for it.

Note: For information about password requirements, see *Table 6* on page 207.

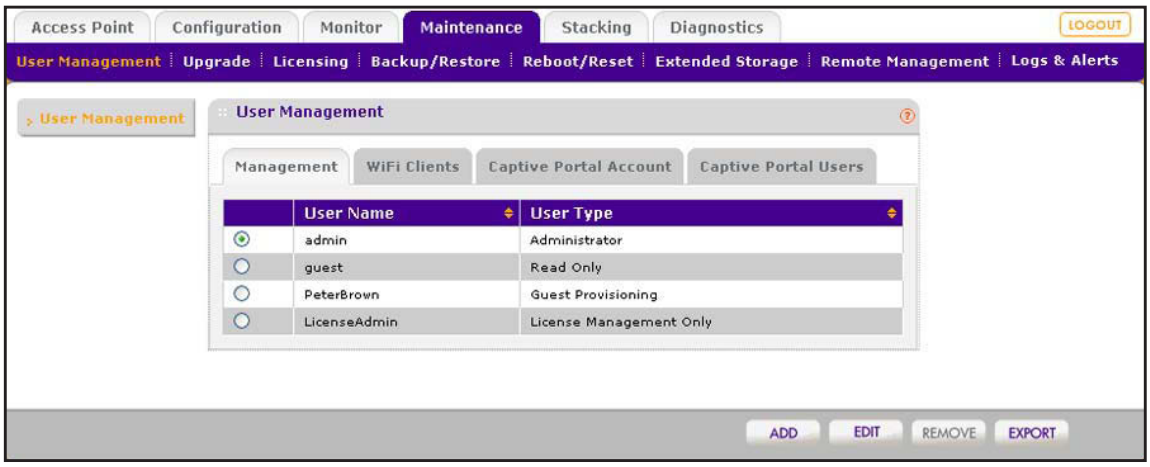
Add a Management User

You can add an administrator, a user who has read-only access to the wireless controller's web management interface, a user who can provision captive portal users only, and a user who can manage licenses only.

➢ **To add a management user:**

1. Select **Maintenance > User Management**.

The User Management screen displays with the Management tab and associated screen in view. The following figure contains some account examples.



2. Click **Add**.

   The Add User pop-up screen displays.

3. Configure the user settings as described in the following table.

Setting	Description
User Name	Enter a unique user name. Only alphanumerical characters and underscore characters (_) are supported.
User Type	From the menu, select the type of user, which determines the users's access to the wireless controller's web management interface. • **Administrator**. Full access with read and write capabilities. • **Read Only**. Read-only access that is restricted to the Monitor and Help main navigation tabs. • **Guest Provisioning**. Access that is restricted to the User Management configuration menu tab under the Maintenance main navigation tab. • **License Management Only**. Access that is restricted to the License configuration menu tab under the Maintenance main navigation tab.
Password	Enter a password in the Password field. Confirm the password in the Confirm Password field.

4. Click **Apply**.

The user is added to the table on the User Management screen.

Add a WiFi Client

You can add a user who is allowed to access the wireless network but who does not need to go through the captive portal or the guest portal.

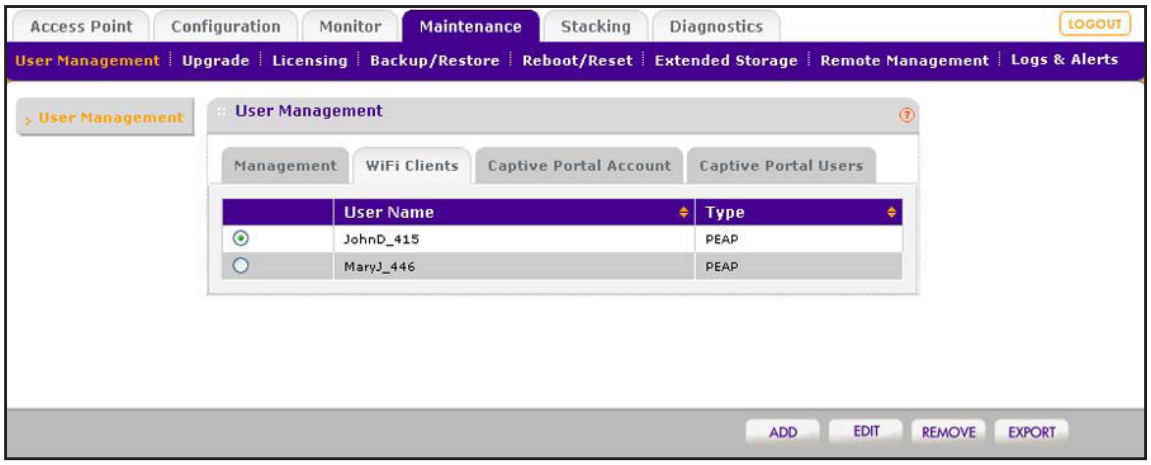
➢ **To add a WiFi client:**

1. Select **Maintenance > User Management**.

   The User Management screen displays with the Management tab and associated screen in view.

2. Click the **WiFi Clients** tab.

   The WiFi Client screen displays. The following figure contains some account examples.



3. Click **Add**.

   The Add User pop-up screen displays.

4. Configure the client settings as described in the following table.

Setting	Description
User Name	Enter a unique user name. Only alphanumerical characters and underscore characters (_) are supported.
Password	Enter a password in the Password field. Confirm the password in the Confirm Password field.
Authentication Type	From the menu, select one of the following protocols: • **EAP**. Extensible Authentication Protocol. • **PEAP**. Protected EAP.

5. Click **Apply**.

   The client is added to the table on the User Management screen.

Add a Captive Portal Account

You can add a captive portal account when you have configured a captive portal but not when you have configured a guest portal. For information about configuring a portal, see *Configure a Portal* on page 113.

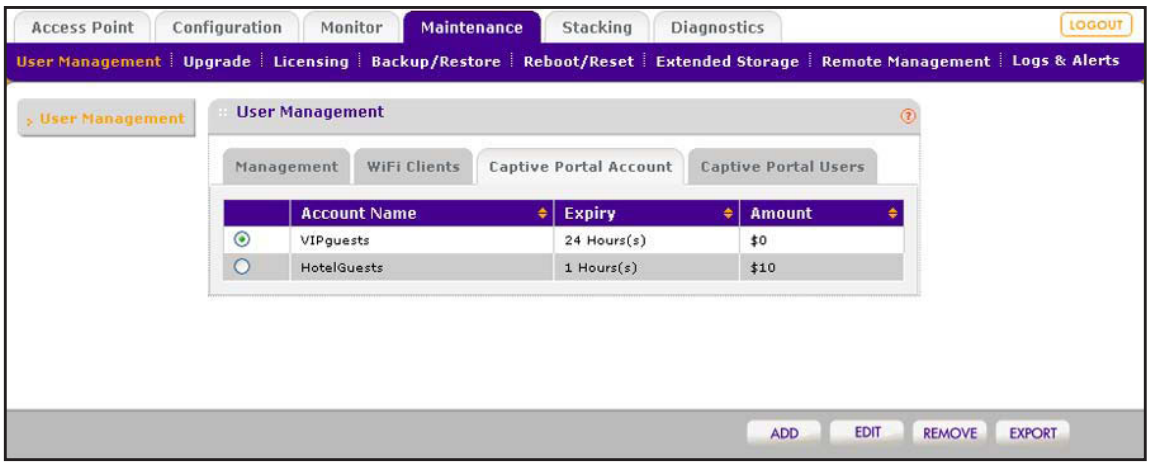
➢ **To add a captive portal account:**

1. Select **Maintenance > User Management**.

   The User Management screen displays with the Management tab and associated screen in view.

2. Click the **Captive Portal Account** tab.

   The Captive Portal Account screen displays. The following figure contains some account examples.



3. Click **Add**.

The Add Account pop-up screen displays.

4. Configure the account settings as described in the following table.

Setting	Description
Account Name	Enter a unique account name. Only alphanumerical characters and underscore characters (_) are supported.
Amount	Enter the total amount that is charged for the period during which access is available. Enter whole numbers only.
Currency Sign	Enter the currency that is associated with the amount.
Expiry	From the menu, select one of the following periods, and enter a valid number in the field to the left of the menu: • **Hour(s)**. The expiration period is measured in one or more hours. • **Day(s)**. The expiration period is measured in one or more days. • **Week(s)**. The expiration period is measured in one or more weeks. • **Month(s)**. The expiration period is measured in one or more months.
Print Message	(Optional) Enter a message for the captive portal user.

5. Click **Apply**.

   The account is added to the table on the User Management screen.

Add a Captive Portal User

You can add a captive portal user when you have configured a captive portal but not when you have configured a guest portal. For information about configuring a portal, see *Configure a Portal* on page 113.

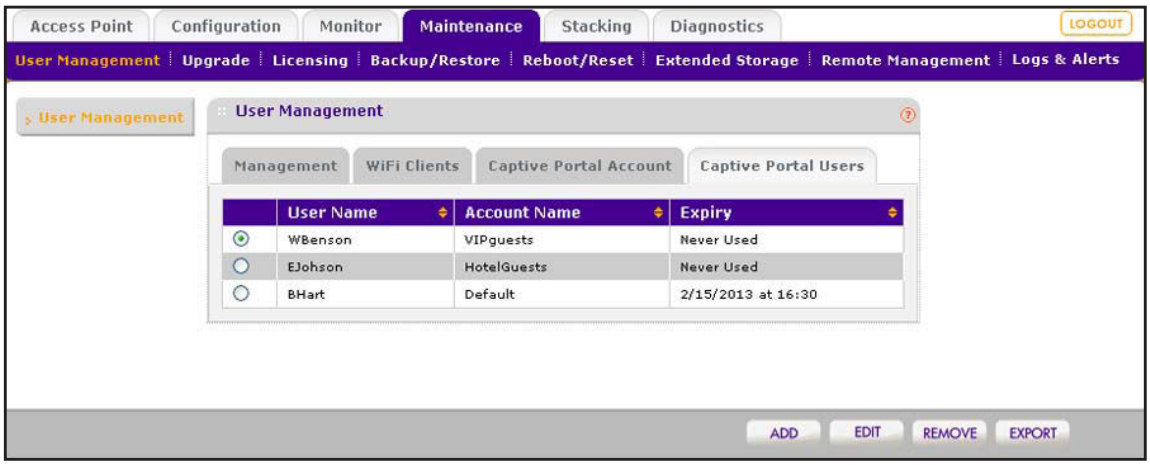
➢ **To add a captive portal user:**

1. Select **Maintenance > User Management**.

   The User Management screen displays with the Management tab and associated screen in view.

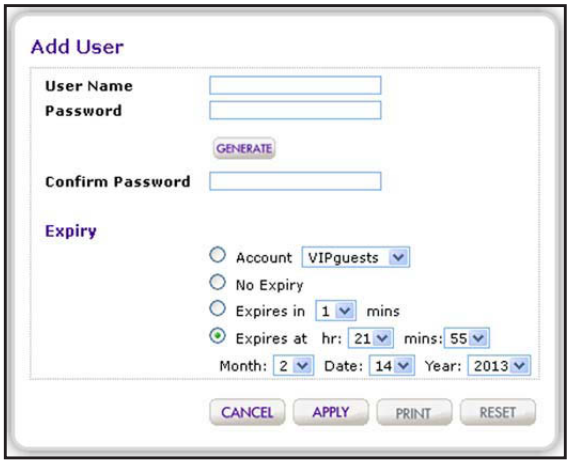
2. Click the **Captive Portal Users** tab.

The Captive Portal Users screen displays. The following figure contains some account examples.



3. Click **Add**.

The Add User pop-up screen displays.



4. Configure the user settings as described in the following table.

Setting	Description
User Name	Enter a unique user name. Only alphanumerical characters and underscore characters (_) are supported.
Password	There are two methods to populate the password fields. Use either one method. Method one: 1. Enter a password in the Password field. 2. Confirm the password in the Confirm Password field. Method two: Click **Generate**. A password is generated automatically.

Setting	Description
Expiry	Select one of the following radio buttons, all of which are mutually exclusive: • **Account**. Select a captive portal account from the menu. Wireless access expires according to the expiration period that is specified for the selected account (see *Add a Captive Portal Account* on page 119). • **No Expiry**. Wireless access does not expire. • **Expires in**. Wireless access expires within one hour. From the mins menu, select in how many minutes access expires. • **Expires at**. Wireless access expires at a date and time that you specify by making selections from the following menus: hr, mins, Month, Date, and Year.

5. (Optional) Click **Print**.

   The user information is printed.

6. Click **Apply**.

   The user is added to the table on the User Management screen.

Edit or Remove a User or Account

You can easily change or remove a user or an account.

➢ **To edit or remove a user or an account:**

1. Select **Maintenance > User Management**.

   The User Management screen displays with the Management tab and associated screen in view.

2. Click one of the following tabs:
   - **Management**
   - **WiFi Clients**
   - **Captive Portal Account**
   - **Captive Portal Users**
3. Select the radio button that corresponds to the user or account that you want to edit or remove.
4. Click one of the following buttons:
   - **Edit**. Opens a pop-up screen that lets you change the user or account settings.
   - **Remove**. Removes the user from the user table.

   Note: *You cannot remove a captive portal account that has one or more captive portal users associated with it. You first need to assign the users to another account, and then you can remove the account.*

5. (Applies only when you have edited user or account settings) Click **Apply**.

   The settings are saved in the table on the User Management screen.

Export a List of Users or Accounts

You can export a list of users or account as a comma-separated values (CSV) file.

➢ **To export a list of users or accounts:**

1. Select **Maintenance > User Management**.

   The User Management screen displays with the Management tab and associated screen in view.

2. Click one of the following tabs:
   - **Management**
   - **WiFi Clients**
   - **Captive Portal Account**
   - **Captive Portal Users**
3. Click **Export**.

   The selected list is opened or saved as a zipped CSV file to a location that you specify.

4. Follow the directions of your browser to complete the procedure.

Configure Wireless and QoS Settings

8

This chapter includes the following sections:

- *Basic and Advanced Wireless and QoS Configuration Concepts*
- *Configure the Radio*
- *Configure Wireless Settings*
- *Configure Channels*
- *Specify RF Management*
- *Configure QoS for Advanced Profile Groups*
- *Configure Load Balancing*
- *Configure Rate Limiting*

Basic and Advanced Wireless and QoS Configuration Concepts

It is important to know how to configure your network and decide which configuration model better fits your needs, basic or advanced. Once you follow one, it is easy to use the same configuration model for the wireless and Quality of Service (QoS) settings. Before you configure the wireless settings, read *Basic and Advanced Setting Concepts* on page 20.

- **Basic wireless settings**. If you use the basic configuration model, the following wireless and QoS settings apply to all profiles in the basic profile group:
  - Basic radio on/off schedule
  - Basic wireless settings for each radio in the basic profile
  - Basic RF management
  - Basic rate limiting for each radio in the basic profile
- **Advanced wireless settings**. If you use the advanced configuration model, you can configure the following wireless and QoS settings separately for each profile group that you have created:
  - Advanced radio on/off schedules for up to eight profile groups
  - Advanced wireless settings for each radio in up to eight profile groups
  - Advanced QoS settings for each radio in up to eight profile groups
  - Advanced RF management for up to eight profile groups
  - Advanced rate limiting for each radio in up to eight profile groups
- **Global wireless settings**. The following wireless and QoS settings apply to all profiles, whether in the basic profile group or in any of the advanced profile groups:
  - Basic channel allocation
  - Basic load balancing for each type of access point model

Configure the Radio

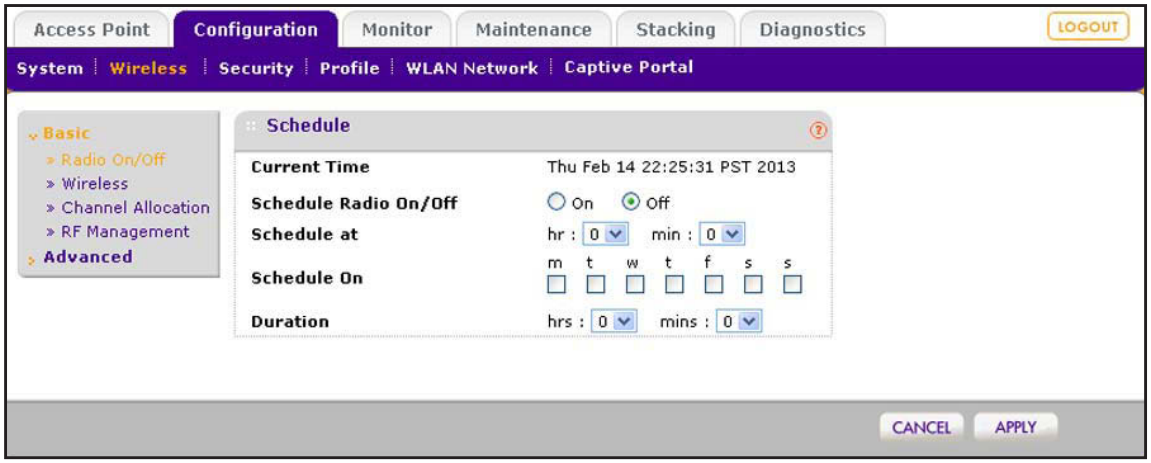
Radio On/Off is a green feature that can be used during scheduled vacations or plant shutdowns, on evenings, or on weekends.

Configure the Radio for the Basic Profile Group

➢ **To schedule the radio for the basic profile group:**

1. Select **Configuration > Wireless > Basic > Radio On/Off**.

   The basic Schedule screen displays:



2. Configure the settings as described in the following table:

Setting	Description
Current Time	This is a nonconfigurable field that displays the current time for the wireless controller.
Schedule Radio On/Off	You can specify either when the radio is on by selecting the **On** radio button or when it is off by selecting the **Off** radio button.
Schedule at	From the menus, specify the time (hours and minutes) when you want to turn the radio either on or off.
Schedule On	Select the check boxes for each day of the week that you want to schedule the radio to be either on or off.
Duration	From the menus, specify the duration (in hours and minutes) that the radio should be either on or off.

3. Click **Apply**.

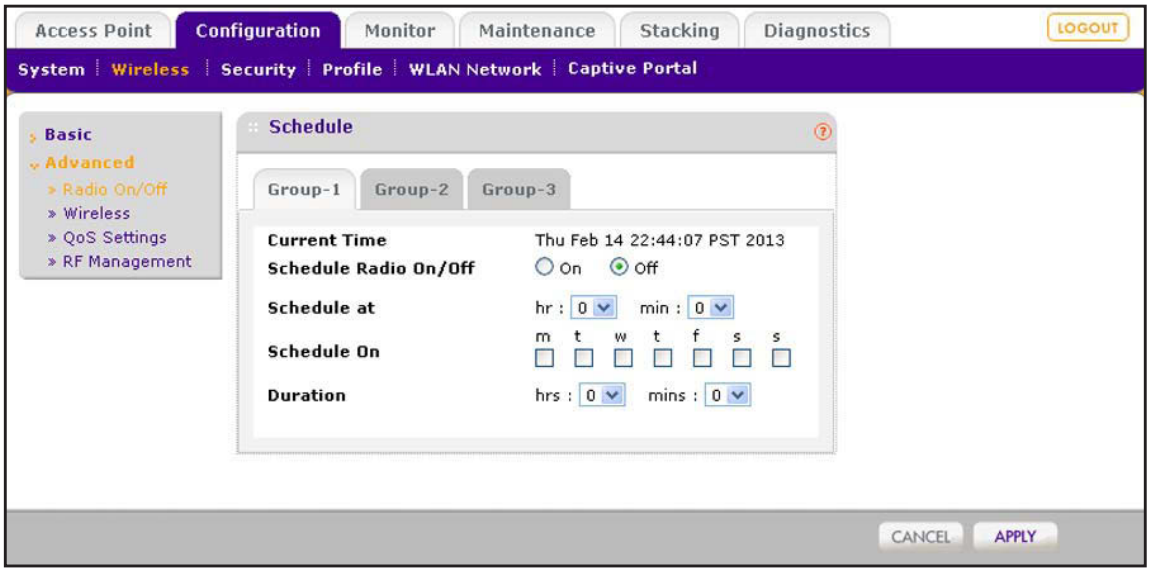
Configure the Radio for an Advanced Profile Group

You can schedule the radio for specific groups to match their network usage. For example, during registration, a school could leave the radios on for the main office or administration building, and turn off radios in buildings that contain only classrooms that are not in use.

➢ **To schedule the radio for an advanced profile group:**

1. Select **Configuration > Wireless > Advanced > Radio On/Off**.

   The advanced Schedule screen displays:



2. Click the tab for the profile group for which you want to configure the radio.
3. Configure the settings as described in the following table:

Setting	Description
Current Time	This is a nonconfigurable field that displays the current time for the wireless controller.
Schedule Radio On/Off	You can specify either when the radio is on by selecting the **On** radio button or when it is off by selecting the **Off** radio button.
Schedule at	From the menus, specify the time (hours and minutes) when you want to turn the radio either on or off.
Schedule On	Select the check boxes for each day of the week that you want to schedule the radio to be either on or off.
Duration	From the menus, specify the duration (in hours and minutes) that the radio should be either on or off.

4. Click **Apply**.

Configure Wireless Settings

During initial setup, you entered your country and region in the General Settings screen (see *Configure General Settings* on page 47). Based on your location and environment, the wireless controller determined the best wireless settings for the discovered access points and pushed these settings to your managed access points.

IMPORTANT:

Unless your network and environment require that you use other wireless settings, NETGEAR recommends that you leave the wireless settings as they are.

Typically, the default wireless settings do not need adjustment. Override the wireless settings only if there is a specific need, such as a phone vendor that specifies a setting different from the default. You can configure wireless settings for the basic profile group and for advanced profile groups (see *Configure Wireless Settings for an Advanced Profile Group* on page 133).

Configure Wireless Settings for the Basic Profile Group

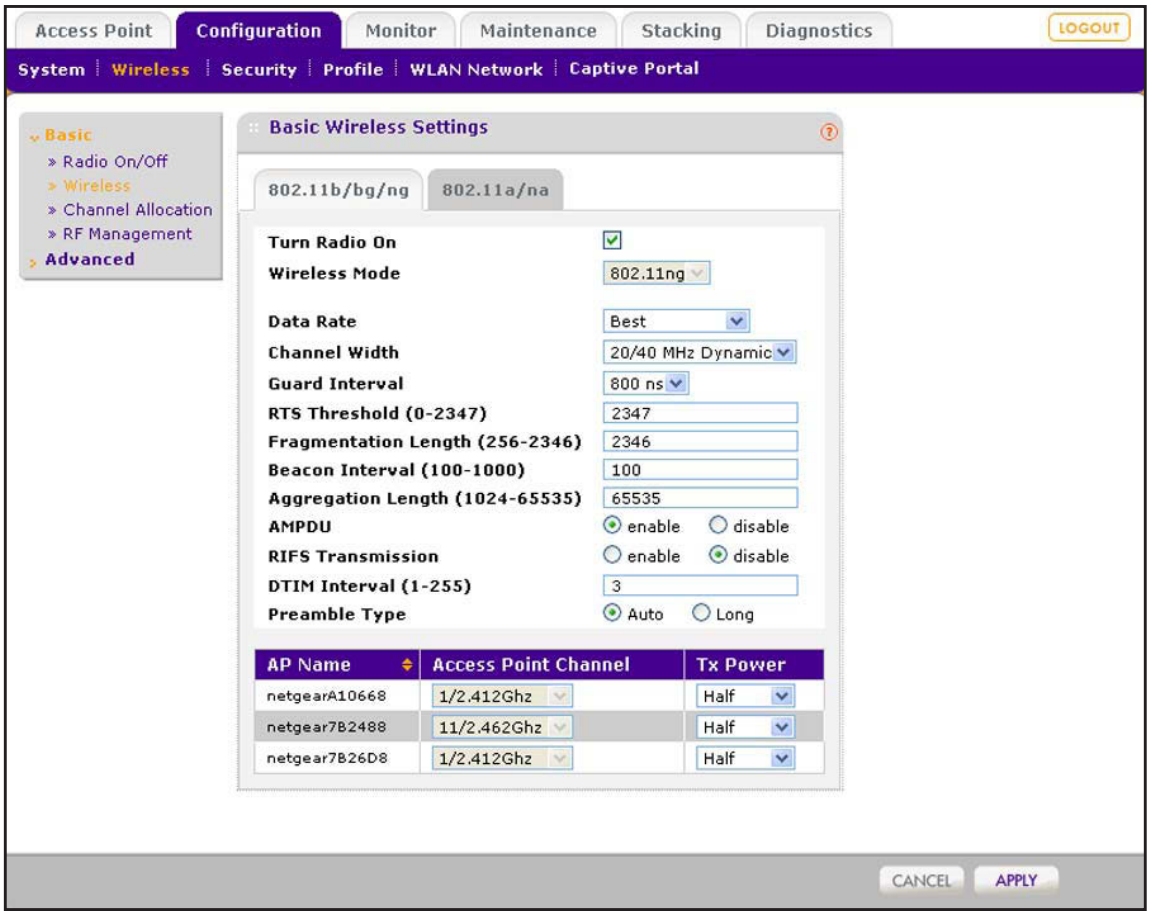
There are two requirements for you to be able to configure the wireless settings on the Basic Wireless Settings screen:

- You need to disable automatic channel allocation for the radio on the Channel Allocation screen. For information about channel allocation, see *Configure Channels* on page 137.
- There needs to be at least one access point assigned to the profile group for the radio for which you want to configure the wireless settings.

➢ **To configure wireless settings for the basic profile group:**

1. Select **Configuration > Wireless > Basic > Wireless**.

The Basic Wireless Settings screen displays:



2. Click the tab for the radio for which you want to configure the wireless settings.
3. Select the **Turn Radio On** check box.

   The wireless settings become accessible and you can configure them. If you cannot select the Turn Radio On check box, see the requirements are the beginning of this section.

4. Configure the settings as described in the following table:

Setting	Description
Wireless Mode	The selections that are available depend on the selected radio mode. From the menu select the wireless mode: • 802.11b/bg/ng mode: - **11ng**. This is the default setting. - **11bg**. - **11b**. • 802.11a/na mode: - **11na**. This is the default setting. - **11a**. **Note:** If you select 802.11bg or 802.11b mode, both 802.11n- and 802.11g-compliant devices can connect to the access points. However, if you select 802.11ng mode, 802.11b-compliant devices cannot connect.
Data Rate	From the menu, select the available transmit data rates of the wireless network.
Channel Width (802.11n only)	From the menu, select the channel width: • **20 MHz Static**. • **20/40 MHz Dynamic**. This is the default setting. A wider channel improves the performance, but some legacy devices can operate only with a 20 MHz channel width.
Guard Interval (802.11n only)	From the menu, select a value that protects transmissions from interference. A shorter guard interval improves performance, but some legacy devices can operate only with a long guard interval.
RTS Threshold (0-2347)	Enter the size of the Request to Send (RTS) threshold packet. The RTS threshold is related to the transmission mechanism (CSMA/CA or CSMA/CD) for the packets. If the packet size is equal to or less than this threshold, the data frame is transmitted immediately; if the packet size is larger than the specified value, the transmitting station needs to send an RTS threshold packet to the receiving station, and then should wait for the receiving station to return a Clear to Send (CTS) packet before sending the actual packet data.
Fragmentation Length (256-2346)	Enter the size that specifies the maximum fragmentation length for data packets. Packets larger than the specified fragmentation length are broken up into smaller packets before being transmitted. The fragmentation length needs to be an even number.
Beacon Interval (100-1000)	Enter the time interval for each beacon transmission that allows the access point to synchronize the wireless network.
Aggregation Length (1024-65535) (802.11n only)	Enter the maximum length of aggregated MAC protocol data unit (AMPDU) packets. Larger aggregation lengths can lead to better network performance. Aggregation is a mechanism used to achieve higher throughput.

Setting	Description
AMPDU (802.11n only)	Select the **On** radio button to allow the aggregation of several MAC frames into a single large frame to achieve higher throughput. Enabling AMPDU can lead to better network performance. Select the **Off** radio button to disable this option.
RIFS Transmission (802.11n only)	Select the **On** radio button to enable the reduced interframe space (RIFS) option to allow transmission of successive frames at different transmit powers. Enabling RIFS can lead to better network performance. Select the **Off** radio button to disable this option.
DTIM Interval (1-255)	Enter the delivery traffic indication message (DTIM) or the data beacon rate that you want to use. This sets the message period of the beacon delivery traffic indication in multiples of beacon intervals.
Preamble Type (802.11b/bg only)	Select one of the following radio buttons to specify the preamble type: • **Auto**. Automatically handles both long and short preambles. A short transmit preamble provides better performance. Auto is the default setting. • **Long**. Enables a long transmit preamble to provide a more reliable connection or a slightly longer range.

5. Click **Apply**.

Override Channel and Transmission Power in the Basic Profile Group

The table on the Basic Wireless Settings screen shows the access points that are managed in the profiles of the basic profile group and to which the channel allocation and basic RF management settings apply.

After you have configured the wireless settings for the basic profile group (see the previous section), you can change the channel, the transmission power, or both for individual access points in the basic profile group.

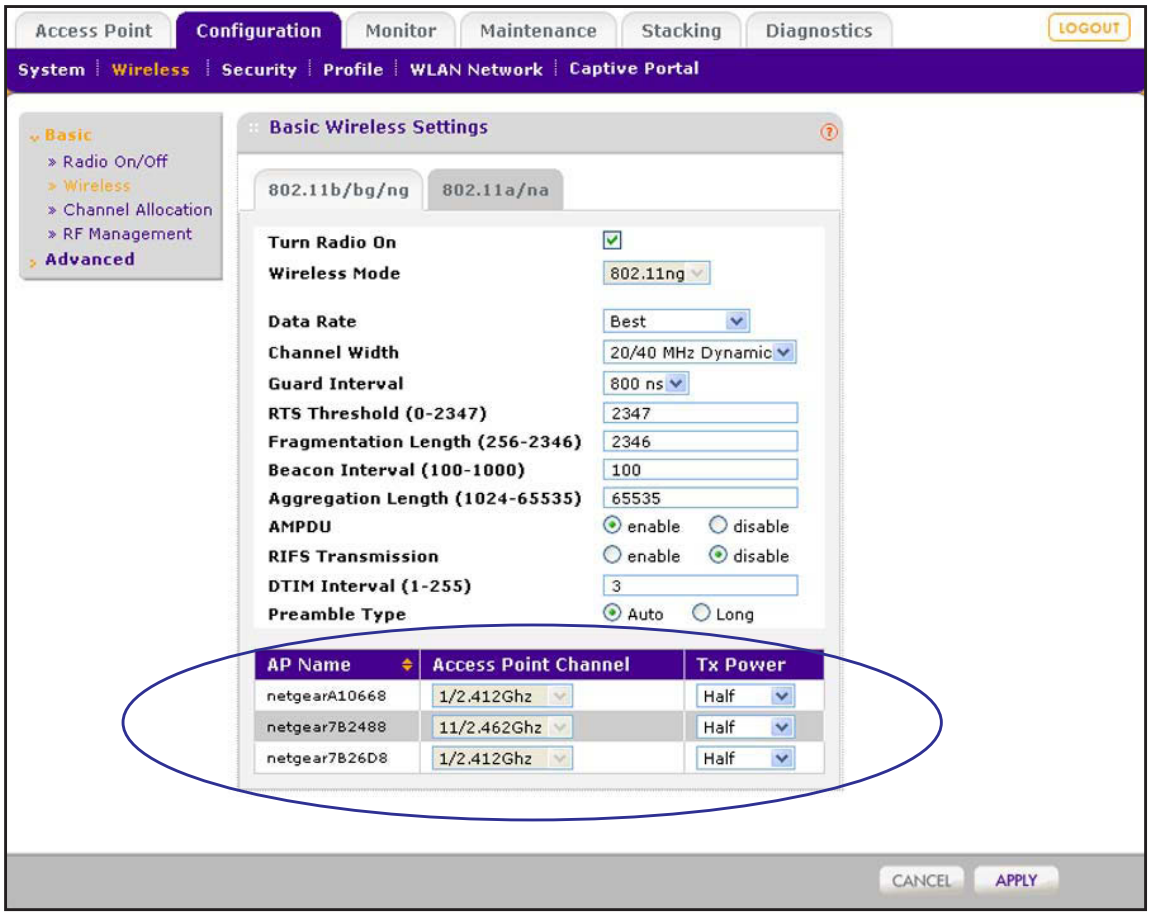
For you to be able to configure these settings in the table, there are two requirements:

- **Channel**. To enable the Access Point Channel menu in the table, you need to disable automatic channel allocation on the Channel Allocation screen (see *Configure Channels* on page 137).
- **Transmission power**. To enable the Tx Power menu in the table, you need to disable automatic Tx power control on the basic RF Management screen (see *RF Management for the Basic Profile Group* on page 141).

➢ **To override the channel and transmission power for individual access points in a security profile of the basic profile group:**

1. Select **Configuration > Wireless > Basic > Wireless**.

The Basic Wireless Settings screen displays.



2. Click the tab for the radio for which you want to configure the wireless settings.
3. Configure the settings in the table at the bottom of the screen as described in the following table:

Setting	Description
AP Name	The name of the access point.
Access Point Channel	Override these settings only if there is a specific need. From the menu, select a channel and frequency for the access point to operate in. **Note:** Changing a channel might temporarily affect the traffic on the access point. **Note:** By default, the access point's channel and frequency are set to the ones that are enabled for the radio and profile group. If the channel and frequency are not available on the access point, the channel and frequency are set to the ones providing the highest performance. For more information, see *Configure Channels* on page 137.

Setting	Description
Tx Power	From the menu, select the transmission power of the access point. **Note:** By default, the access point's transmission power is set to the configuration that is selected on the basic RF Management screen. For more information, see *RF Management for the Basic Profile Group* on page 141.

4. Click **Apply**.

Configure Wireless Settings for an Advanced Profile Group

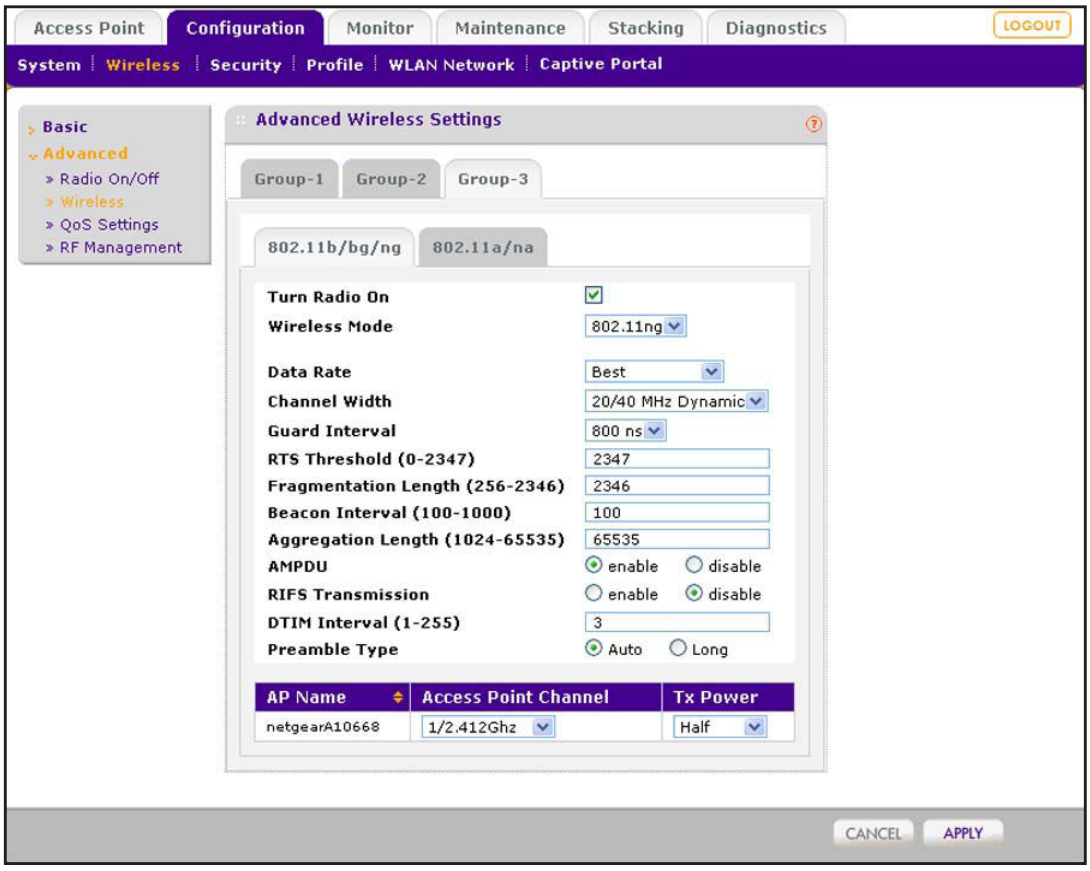
There are two requirements for you to be able to configure the wireless settings on the Advanced Wireless Settings screen:

- You need to disable automatic channel allocation for the radio on the Channel Allocation screen. For information about channel allocation, see *Configure Channels* on page 137.
- There needs to be at least one access point assigned to the profile group for the radio for which you want to configure the wireless settings.

➢ **To configure wireless settings for an advanced profile group:**

1. Select **Configuration > Wireless > Advanced > Wireless**.

   The Advanced Wireless Settings screen displays:



2. Click the tab for the profile group for which you want to configure the wireless settings.
3. Click the tab for the radio for which you want to configure the wireless settings.
4. Select the **Turn Radio On** check box.

   The wireless settings become accessible and you can configure them. If you cannot select the Turn Radio On check box, see the requirements are the beginning of this section.
5. Configure the settings as described in the following table:

Setting	Description
Wireless Mode	The selections that are available depend on the selected radio mode. From the menu select the wireless mode: • 802.11b/bg/ng mode: - **11ng**. This is the default setting. - **11bg**. - **11b**. • 802.11a/na mode: - **11na**. This is the default setting. - **11a**. **Note:** If you select 802.11bg or 802.11b mode, both 802.11n- and 802.11g-compliant devices can connect to the access points. However, if you select 802.11ng mode, 802.11b-compliant devices cannot connect.
Data Rate	From the menu, select the available transmit data rates of the wireless network.
Channel Width (802.11n only)	From the menu, select the channel width: • **20 MHz Static**. • **20/40 MHz Dynamic**. This is the default setting. A wider channel improves the performance, but some legacy devices can operate only with a 20 MHz channel width.
Guard Interval (802.11n only)	From the menu, select a value that protects transmissions from interference. A shorter guard interval improves performance, but some legacy devices can operate only with a long guard interval.
RTS Threshold (0-2347)	Enter the size of the Request to Send (RTS) threshold packet. The RTS threshold is related to the transmission mechanism (CSMA/CA or CSMA/CD) for the packets. If the packet size is equal to or less than this threshold, the data frame is transmitted immediately; if the packet size is larger than the specified value, the transmitting station needs to send an RTS threshold packet to the receiving station, and then should wait for the receiving station to return a Clear to Send (CTS) packet before sending the actual packet data.

Setting	Description
Fragmentation Length (256-2346)	Enter the size that specifies the maximum fragmentation length for data packets. Packets larger than the specified fragmentation length are broken up into smaller packets before being transmitted. The fragmentation length needs to be an even number.
Beacon Interval (100-1000)	Enter the time interval for each beacon transmission that allows the access point to synchronize the wireless network.
Aggregation Length (1024-65535) (802.11n only)	Enter the maximum length of aggregated MAC protocol data unit (AMPDU) packets. Larger aggregation lengths can lead to better network performance. Aggregation is a mechanism used to achieve higher throughput.
AMPDU (802.11n only)	Select the **On** radio button to allow the aggregation of several MAC frames into a single large frame to achieve higher throughput. Enabling AMPDU can lead to better network performance. Select the **Off** radio button to disable this option.
RIFS Transmission (802.11n only)	Select the **On** radio button to enable the reduced interframe space (RIFS) option to allow transmission of successive frames at different transmit powers. Enabling RIFS can lead to better network performance. Select the **Off** radio button to disable this option.
DTIM Interval (1-255)	Enter the delivery traffic indication message (DTIM) or the data beacon rate that you want to use. This sets the message period of the beacon delivery traffic indication in multiples of beacon intervals.
Preamble Type (802.11b/bg only)	Select one of the following radio buttons to specify the preamble type: • **Auto**. Automatically handles both long and short preambles. A short transmit preamble provides better performance. Auto is the default setting. • **Long**. Enables a long transmit preamble to provide a more reliable connection or a slightly longer range.

6. Click **Apply**.

Override Channel and Transmission Power in an Advanced Profile Group

The table on the Advanced Wireless Settings screen shows the access points that are managed in the profiles of an advanced profile group and to which the channel allocation and advanced RF management settings apply.

After you have configured the wireless settings for an advanced profile group (see the previous section), you can change the channel, the transmission power, or both for individual access points in an advanced profile group.

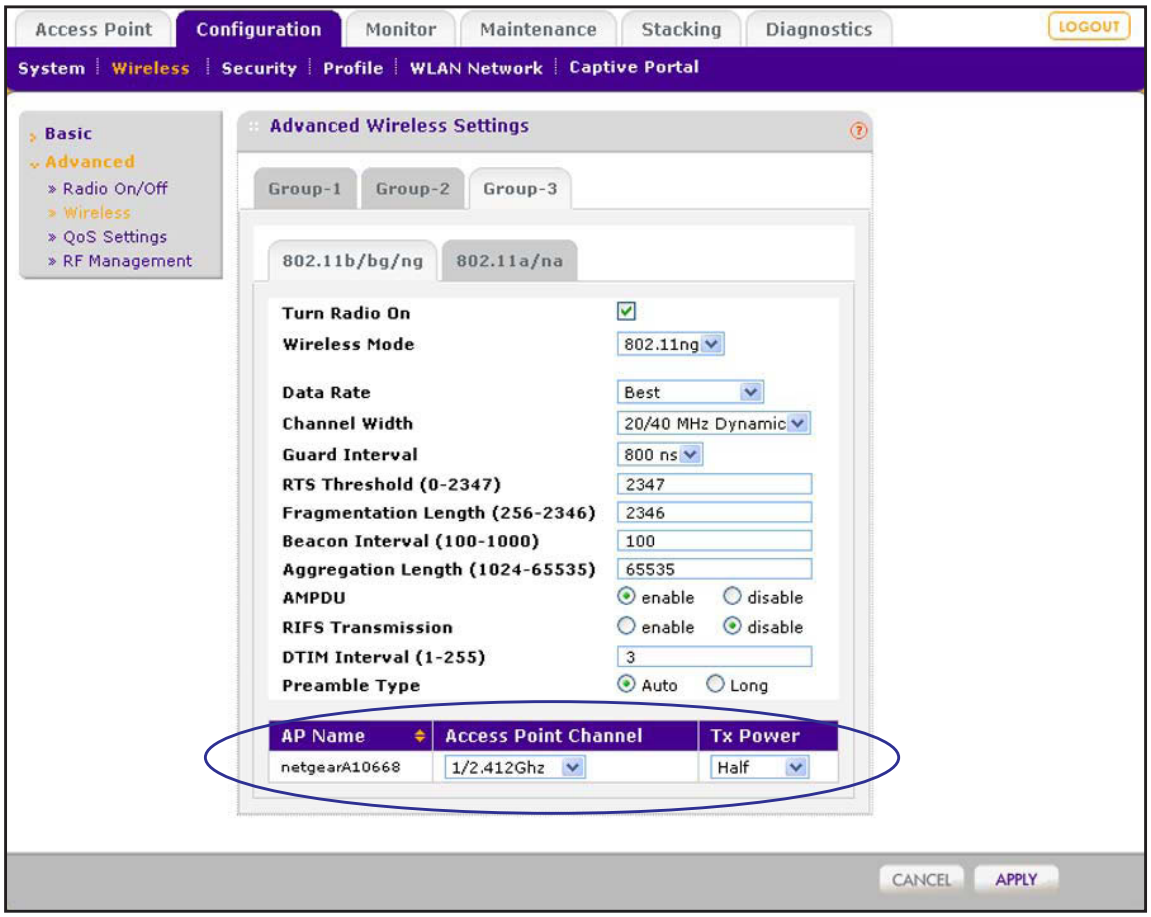
For you to be able to configure these settings in the table, there are two requirements:

- **Channel**. To enable the Access Point Channel menu in the table, you need to disable automatic channel allocation on the Channel Allocation screen (see *Configure Channels* on page 137).
- **Transmission power**. To enable the Tx Power menu in the table, you need to disable automatic Tx power control on the advanced RF Management screen (see *RF Management for an Advanced Profile Group* on page 142).

➢ **To override the channel and transmission power for individual access points in a security profile of an advanced profile group:**

1. Select **Configuration > Wireless > Advanced > Wireless**.

   The Advanced Wireless Settings screen displays.



2. Click the tab for the profile group for which you want to configure the wireless settings.
3. Click the tab for the radio for which you want to configure the wireless settings.

4. Configure the settings in the table at the bottom of the screen as described in the following table.

Setting	Description
AP Name	The name of the access point.
Access Point Channel	Override these settings only if there is a specific need. From the menu, select a channel and frequency for the access point to operate in. **Note:** Changing a channel might temporarily affect the traffic on the access point. **Note:** By default, the access point's channel and frequency are set to the ones that are enabled for the radio and profile group. If the channel and frequency are not available on the access point, the channel and frequency are set to the ones providing the highest performance. For more information, see *Configure Channels* on page 137.
Tx Power	From the menu, select the transmission power of the access point. **Note:** By default, the access point's transmission power is set to the configuration that is selected on the basic RF Management screen. For more information, see *RF Management for an Advanced Profile Group* on page 142.

5. Click **Apply**.

Configure Channels

CAUTION:

Do not disable channel allocation unless you are debugging or there is an extreme situation that affects the channels.

Automatic channel allocation distributes channels across the managed access points to reduce interference. Each wireless controller allocates channels for its managed access points, regardless of their configured security profiles. The wireless controller detects interference, traffic load on the access point, and neighborhood maps to determine the best channel for an access point. This information, collected over the previous 24 hours, is used by the wireless controller to determine the best possible channel for the access point.

You can configure channel allocation to allow allocation of only the specified channels when channel allocation is scheduled to run. This ensures that the access points use only the channels allowed according to administration policies.

To adhere to best practices when adjusting channel allocation, NETGEAR recommends the following:

- Select channels that do not overlap. For example, for 2.4 GHz, use channels 1, 6, and 11.
- Schedule channel allocation once a day at times when the fewest clients are expected to be connected. This allows better management of available bandwidth during the day.

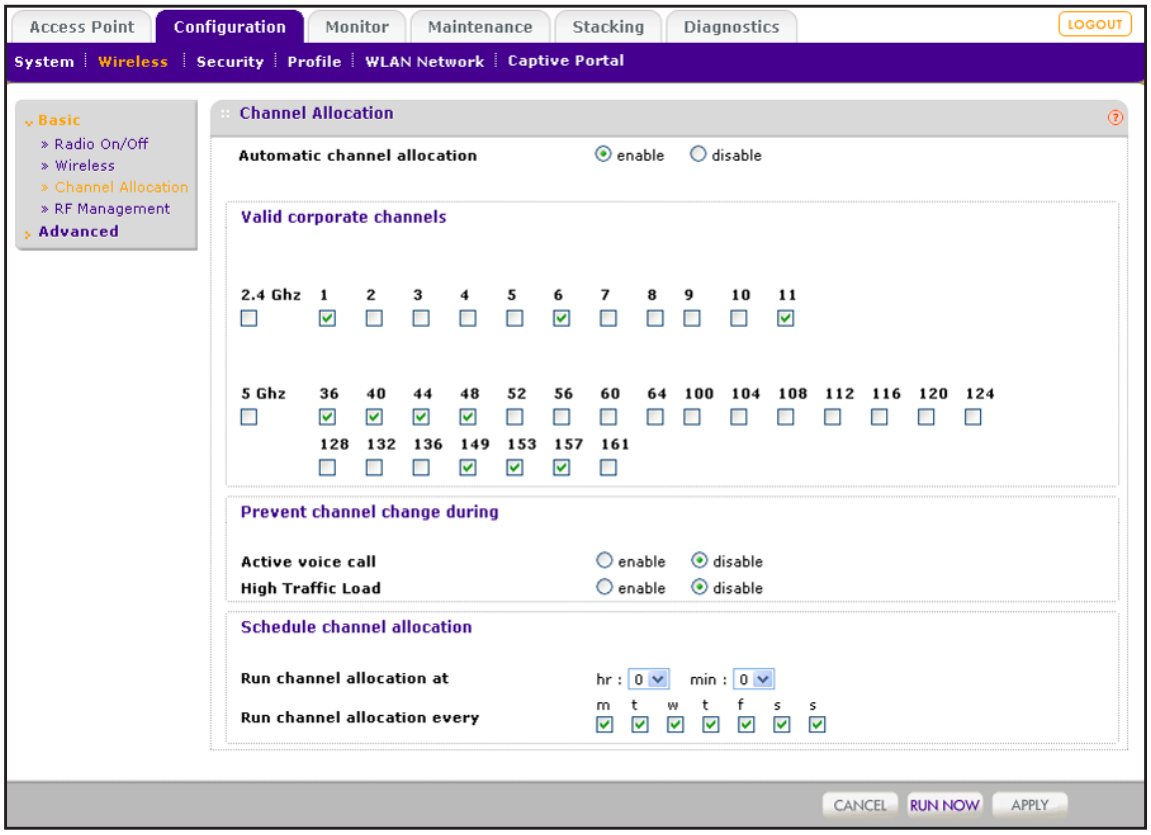
The allocated channels apply to all access points, irrespective of whether they are managed in profiles of the basic profile group or profiles of an advanced profile group. However, you *can* override the general channel allocation settings for individual access points on the Basic Wireless Settings screen and on the Advanced Wireless Settings screen. For more information, see:

- *Override Channel and Transmission Power in the Basic Profile Group*
- *Override Channel and Transmission Power in an Advanced Profile Group*

➢ **To change the channel allocation:**

1. Select **Configuration > Wireless > Basic > Channel Allocation**.

   The Channel Allocation screen displays:



2. Configure the settings as described in the following table:

Setting	Description	
Automatic channel allocation	Ensure that the **enable** radio button is selected during normal operation. Automatic channel allocation distributes channels across the managed access points to reduce interference. To disable automatic channel allocation, select the **disable** radio button.	
Valid corporate channels	Specify the wireless band by selecting the **2.4 GHz** or **5 GHz** check box. For each wireless band, the following applies: • You can remove one or more channels from the list of available channels by clearing their check boxes. This is a good way to avoid interference with competing equipment such as in a medical setting where medical devices use a specific channel. • You cannot add channels. The wireless controller determines available channels based on the country or region that you specified on the General Settings screen (see *Configure General Settings* on page 47).	
Prevent channel change during **Note:** If the wireless controller is prevented from reallocating a channel because it is in use, the wireless controller checks again at the next scheduled channel allocation.	Active voice call	Select the **enable** radio button to prevent channel changes during voice calls. Select the **disable** radio button to allow channel changes during voice calls. This is the default setting.
	High Traffic Load	Select the **enable** radio button to prevent channel changes during a high traffic load. Select the **disable** radio button to allow channel changes during a high traffic load. This is the default setting.
Schedule channel allocation **Note:** NETGEAR recommends that you schedule channel allocation once a day at times when the fewest clients are expected to be connected.	Run channel allocation at	From the menus, select the hour and minutes when the channel allocation should run.
	Run channel allocation every	Select the check boxes to specify the day or days when the channel allocation should run.

IMPORTANT:

Changing channels might temporarily affect traffic on the managed access points in the network.

3. (Optional) Click **Run Now**.

   The channel allocation occurs immediately and the selected channels are applied to the managed access points. This option is useful when you add a new access point or change your network.

4. Click **Apply**.

   If enabled, the channel allocation occurs according to the configured schedule.

Specify RF Management

RF management optimizes the channel allocation for access points based on clients, user data traffic, and the nearby RF environment of access points. The wireless controller periodically checks the radio neighborhood maps and detects changes in the radio neighborhood maps or loss of connectivity to the wireless controller by an access point.

WLAN healing is a special feature of RF management. When WLAN healing is used, if an access point goes down or loses connectivity, other access points share its load to avoid a coverage hole. To do this, the other access points increase their transmit power. WLAN healing is configured per security profile group and is active among access points that share a common security configuration.

You can configure centralized RF management for the basic profile group on the basic RF Management screen. If you use advanced profile groups, you can use the advanced RF Management screen to customize settings for each advanced profile group.

WLAN Healing

The wireless controller has the capacity for automatic WLAN healing through the following features:

- **Automatic channel allocation**. Allows an access point channel to be distributed automatically by the wireless controller across the access points on a floor to reduce interference. Automatic channel allocation considers interference and the traffic load on the access point, as well as the wireless mode and bandwidth (also referred to as channel width) to provide the best channel for the access point. For information about how to configure automatic channel allocation, including the option to skip automatic channel allocation if there is a heavy traffic load or voice activity, see *Configure Channels* on page 137.
- **Automatic transmission power**. Automatically determines the optimum transmit power of an access point based on the coverage requirement. The access point scans its neighborhood to determine the RF environment to minimize neighboring access point interference, leakage across floors, and coverage holes.

When you configure WLAN healing, NETGEAR recommends the following:

- Configure the WLAN self-healing wait time to a value greater than the access point reboot time, which is usually one minute. This allows for fluctuations in the power of nearby access points when access points are rebooted.
- The number of neighbors to participate in WLAN self-healing should not be very large (three to four usually suffices in most deployments). This avoids too many access points increasing power for a single failed access point.

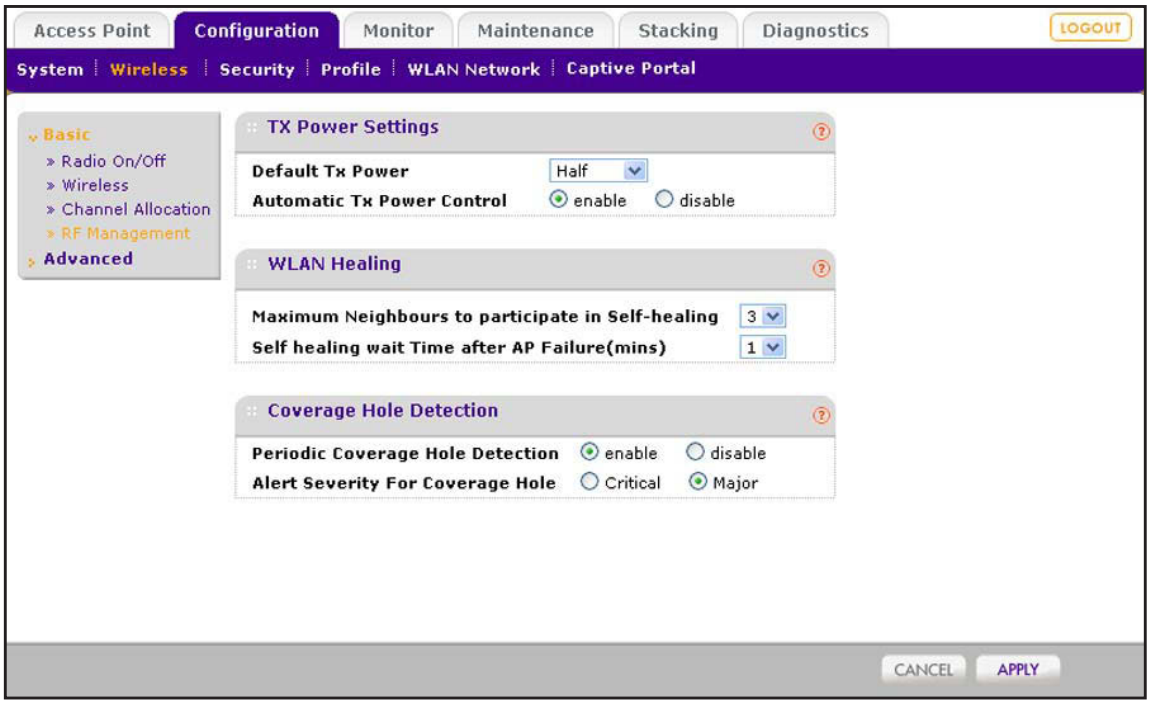
RF Management for the Basic Profile Group

The basic RF Management screen lets you configure the wireless transmission power, WLAN healing, and wireless coverage hole detection for the basic profile group.

➢ **To configure RF management for access points in the basic profile group:**

1. Select **Configuration > Wireless > Basic > RF Management**.

   The basic RF Management screen displays:



2. Configure the settings as described in the following table:

Setting	Description
TX Power Settings	
Default Tx Power	Make a selection from the menu to specify how the transmission (Tx) power is configured on the access points: **Full**, **Half**, **Quarter**, **Eighth**, or **Minimum**. When automatic Tx power control is enabled, the selection from the menu is used as the initial power level for the access points.
Automatic Tx Power Control	Select the **enable** radio button to enable automatic Tx power control: • When a client attempts to connect to an access point at low power, the access point's Tx power is automatically increased above the default level. • When there are overlapping coverage areas, the access point's Tx power is automatically decreased below default level. Select the **disable** radio button to disable automatic Tx power control.

Setting	Description
WLAN Healing	
Maximum Neighbors to Participate in Self-healing	From the menu, select the maximum number of neighboring access points that increase or decrease power to cover for a failing access point. Selecting 0 (zero) disables this feature. Use close neighbors, not a distant access point, and do not use all access points.
Self healing wait Time after AP Failure	From the menu, select the number of minutes to validate (that is, wait) before confirming a failed access point and increasing transmit power to cover the area. Enter a value greater than the access point reboot time, which is usually one minute. This allows for fluctuations in the power of nearby access points when access points are rebooted.
Coverage Hole Detection	
Periodic Coverage Hole Detection	Select the **enable** radio button to allow coverage hole detection to run in the background periodically. Select the **disable** radio button to disable this option.
Alert Severity for Coverage Hole	Select a radio button to specify the type of alarm severity to be associated with a coverage-hole detection event on the Logs & Alerts screen: • **Critical** • **Major** For more information, see *Configure Alarm Notification Settings* on page 61.

3. Click **Apply**.

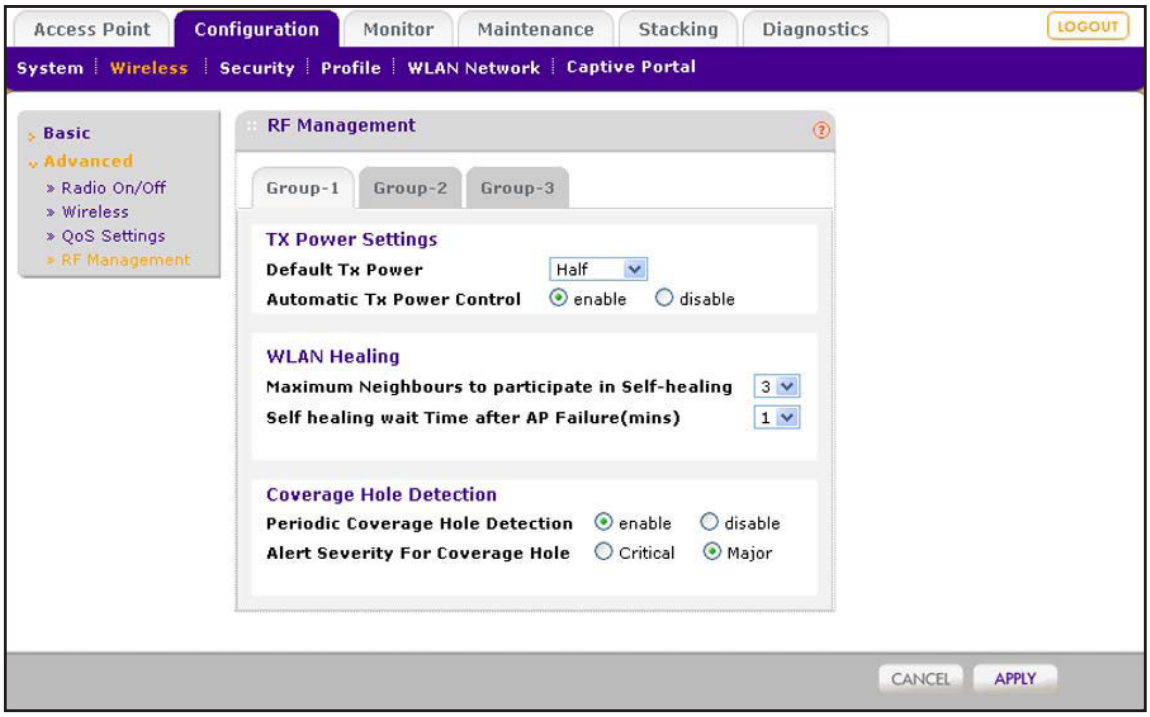
RF Management for an Advanced Profile Group

The advanced RF Management screen lets you configure the wireless transmission power, WLAN healing, and wireless coverage hole detection for advanced profile groups.

➢ **To configure RF management for access points in an advanced profile group:**

1. Select **Configuration > Wireless > Advanced > RF Management**.

The advanced RF Management screen displays:



2. Click the tab for the profile group for which you want to configure RF management.
3. Configure the settings as described in the following table.

Setting	Description
TX Power Settings	
Default Tx Power	Make a selection from the menu to specify how the transmission (Tx) power is configured on the access points: **Full**, **Half**, **Quarter**, **Eighth**, or **Minimum**. When automatic Tx power control is enabled, the selection from the menu is used as the initial power level for the access points.
Automatic Tx Power Control	Select the **enable** radio button to enable automatic Tx power control: • When a client attempts to connect to an access point at low power, the access point's Tx power is automatically increased above the default level. • When there are overlapping coverage areas, the access point's Tx power is automatically decreased below default level. Select the **disable** radio button to disable automatic Tx power control.
WLAN Healing	
Maximum Neighbors to Participate in Self-healing	From the menu, select the maximum number of neighboring access points that increase or decrease power to cover for a failing access point. Selecting 0 (zero) disables this feature. Use close neighbors, not a distant access point, and do not use all access points.

Setting	Description
Self healing wait Time after AP Failure	From the menu, select the number of minutes to validate (that is, wait) before confirming a failed access point and increasing transmit power to cover the area. Enter a value greater than the access point reboot time, which is usually one minute. This allows for fluctuations in the power of nearby access points when access points are rebooted.
Coverage Hole Detection	
Periodic Coverage Hole Detection	Select the **enable** radio button to allow coverage hole detection to run in the background periodically. Select the **disable** radio button to disable this option.
Alert Severity for Coverage Hole	Select a radio button to specify the type of alarm severity to be associated with a coverage-hole detection event on the Logs & Alerts screen: • **Critical** • **Major** For more information, see *Configure Alarm Notification Settings* on page 61.

4. Click **Apply**.

Configure QoS for Advanced Profile Groups

Quality of Service (QoS) works by default for the advanced profile groups. Change QoS only if there is a reason, such as device vendor specifications that require you to use different settings.

Using QoS Wi-Fi MultiMedia (WMM) ensures that the applications that require better throughput and performance are provided special queues with higher priority. For example, video and audio applications are given higher priority over applications such as FTP. WMM defines the following four queues in decreasing order of priority:

- **Voice**. The highest priority queue with minimum delay, which makes it ideal for applications such as voice over IP (VoIP) and streaming media.
- **Video**. The second highest priority queue with low delay is given to this queue. Video applications are routed to this queue.
- **Best Effort**. The medium priority queue with medium delay is given to this queue. Most standard IP applications use this queue.
- **Background**. Low priority queue with high throughput. Applications, such as FTP, that are not time-sensitive but require high throughput can use this queue.

QoS prioritization and coordination of wireless medium access is on. QoS settings on the access point control downstream traffic, flowing from the access point to the client station (*AP* Enhanced Distributed Channel Access [EDCA] parameters) and the upstream traffic flowing from the client station to the access point (*Station* EDCA parameters).

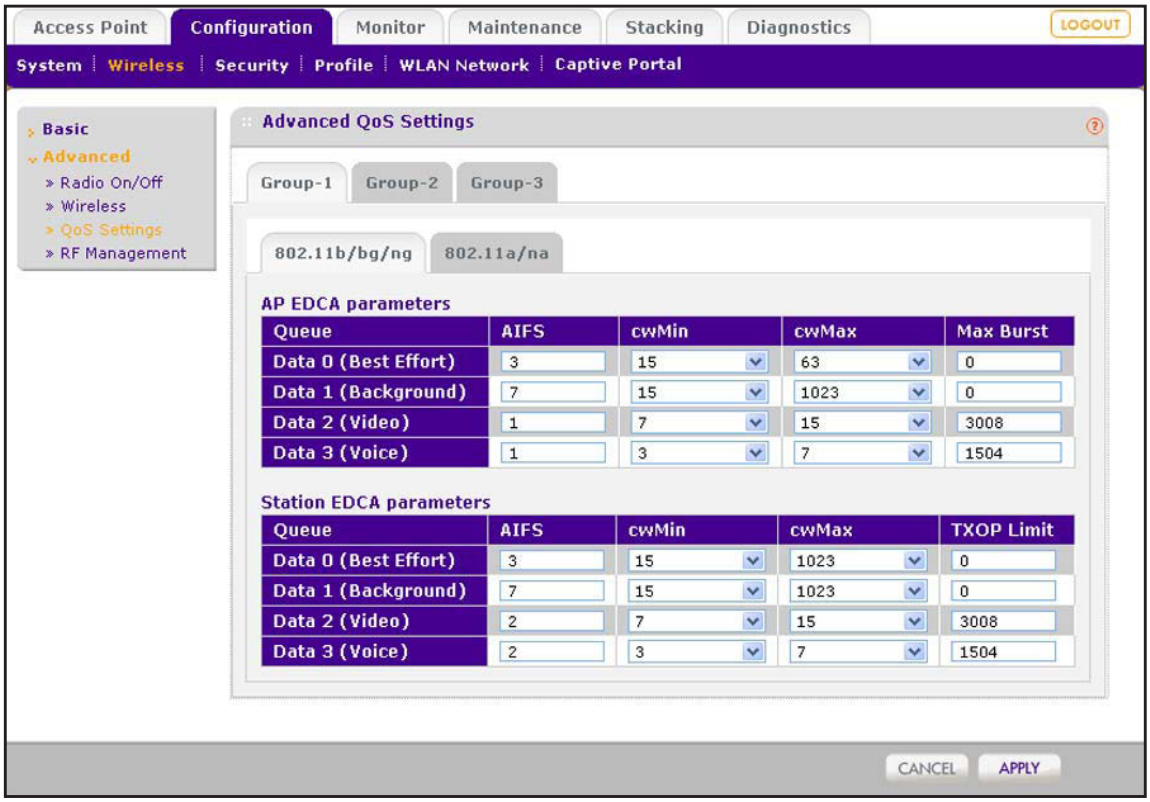
The Advanced QoS Settings screen lets you modify the QoS settings per profile group and per radio for upstream traffic flowing from the station (that is, the wireless client) to managed access points and the downstream traffic flowing from managed access points to the station. These settings are applied only to managed access points that are capable of supporting these settings.

Disabling WMM deactivates QoS control of station EDCA parameters for upstream traffic flowing from the client station to the access point. (You can change the settings for the station EDCA parameters, but these settings do not take effect until you enable WMM.) However, when WMM is disabled, you can still set some parameters for downstream traffic flowing from the access point to the client station (AP EDCA parameters), and these settings do take effect even when WMM is disabled.

➢ **To configure the QoS settings for a profile group:**

1. Select **Configuration > Wireless > Advanced > QoS**.

   The Advanced QoS Settings screen displays:



2. Click the tab for the profile group for which you want to configure the QoS settings.
3. Click the tab for the radio for which you want to configure the QoS settings.
4. Configure the settings as described in the following table:

<table>
<tr><th>Setting</th><th colspan="2">Description</th></tr>
<tr><td rowspan="2">AIFS</td><td colspan="2">Specify a wait time (in milliseconds) for data frames. Valid values for arbitration inter-frame space (AIFS) are 1 through 255.</td></tr>
<tr><td>These are the default values for the AP EDCA parameters:
• Data 0 (Best Effort) 3
• Data 1 (Background) 7
• Data 2 (Video) 1
• Data 3 (Voice) 1</td><td>These are the default values for the Station EDCA parameters:
• Data 0 (Best Effort) 3
• Data 1 (Background) 7
• Data 2 (Video) 2
• Data 3 (Voice) 2</td></tr>
<tr><td rowspan="2">CwMin</td><td colspan="2">Specify an upper limit (in milliseconds) of a range from which the initial random backoff wait time is determined.
Valid values for this field are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1023. The value for the minimum contention window (CwMin) needs to be lower than the value for the maximum contention window (CwMax).</td></tr>
<tr><td>These are the default values for the AP EDCA parameters:
• Data 0 (Best Effort) 15
• Data 1 (Background) 15
• Data 2 (Video) 7
• Data 3 (Voice) 3</td><td>These are the default values for the Station EDCA parameters:
• Data 0 (Best Effort) 15
• Data 1 (Background) 15
• Data 2 (Video) 7
• Data 3 (Voice) 3</td></tr>
<tr><td rowspan="2">CwMax</td><td colspan="2">Specify an upper limit (in milliseconds) for the doubling of the random backoff value.
Valid values for this field are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1023. The value for the maximum contention window (CwMax) needs to be higher than the value for minimum contention window (CwMin).</td></tr>
<tr><td>These are the default values for the AP EDCA parameters:
• Data 0 (Best Effort) 63
• Data 1 (Background) 1023
• Data 2 (Video) 15
• Data 3 (Voice) 7</td><td>These are the default values for the Station EDCA parameters:
• Data 0 (Best Effort) 1023
• Data 1 (Background) 1023
• Data 2 (Video) 15
• Data 3 (Voice) 7</td></tr>
<tr><td rowspan="2">Max Burst
Note: AP EDCA parameters only</td><td colspan="2">Specify (in milliseconds) the maximum burst length allowed for packet bursts on the wireless network.
A packet burst is a collection of multiple frames transmitted without header information. Valid values for maximum burst length are 0.0 through 999.9. The maximum burst length applies only to AP EDCA parameters.</td></tr>
<tr><td colspan="2">These are the default values for the AP EDCA parameters:
• Data 0 (Best Effort) 0
• Data 1 (Background) 0
• Data 2 (Video) 3008
• Data 3 (Voice) 1504</td></tr>
</table>

Setting	Description
TXOP Limit **Note:** Station EDCA parameters only	Specify the transmission opportunity (TXOP) limit. The TXOP limit applies only to station AP EDCA parameters and specifies the maximum period during which the client station client can initiate transmissions.
	These are the default values for the Station EDCA parameters: • Data 0 (Best Effort) 0 • Data 1 (Background) 0 • Data 2 (Video) 3008 • Data 3 (Voice) 1504

5. Click **Apply**.

Configure Load Balancing

Load balancing allows the wireless controller to distribute access point clients (the “load”) equally among the access points that it manages. You configure load balancing per type of access point model and per radio. By default, load balancing is disabled.

When a client discovers an access point using probe requests or sends association frames, the access point determines whether to accept the client based on the number of clients that are already connected, the signal strength of the clients that are already connected, and the signal strength of the client that attempts to connect.

The wireless controller performs load balancing based on the following criteria:

- **Maximum number of clients**. If more than the maximum number of clients per access point attempt to associate, the clients are pushed to another access point.

  When you want a good distribution of clients between the access points, set the maximum number of clients to a low value (compared to, for example, the total number of clients in an office or on a floor).

- **Signal strength or RSSI**. Signal strength determines speed. For a client that is far away from an access point, the data rate is much lower than for a client that is in closer proximity to the access point. The distant client requires more time to transmit or receive data, and the delay could be too long. You can give a threshold for signal strength, which is specified as a percentage, such as 50 percent.

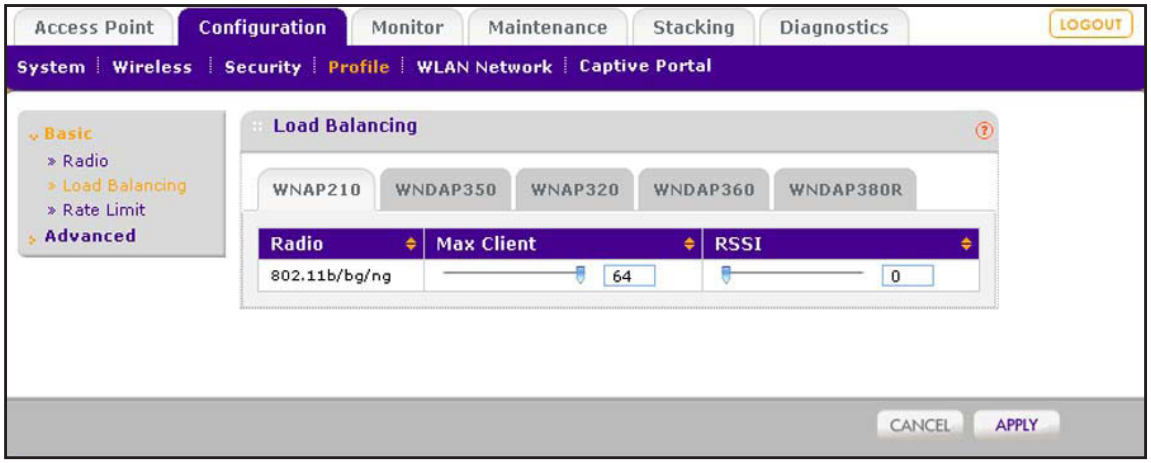
  When you want only clients near an access point to associate with the access point in situations where the throughput expectation is high, set the received signal strength indication (RSSI) to a high percentage. In situations in which the clients can be expected to be far away or there are fewer access points, set the RSSI to a lower value.

Note: The load-balancing settings apply to all profiles, whether they are in the basic profile group or in advanced profile groups.

➢ **To configure load balancing for all access points of one model:**

1. Select **Configuration > Profile > Basic > Load Balancing**.

   The Load Balancing screen displays:



2. Click the tab for the access point model for which you want to configure load balancing.
3. Configure the settings as described in the following table:

Setting	Description
Max Client	Drag the slider to specify or enter the maximum number of wireless clients that can connect to each radio of an access point at one time. You can select a value of 64 to allow the maximum number that is supported by a radio of an access point.
RSSI	Drag the slider to specify or enter the minimum signal quality in percentage (0 to 75 percent) expected from the wireless clients that connect to the access points. A value of 0 means that this check is not enforced and load balancing is disabled.

4. Click **Apply**.

Configure Rate Limiting

The available bandwidth is determined by the number of errors during transmission and the time that a packet spends in the transmission queues.

Within a profile group (including the basic profile group), you configure rate limiting separately for each wireless radio (2.4 GHz and 5 GHz). Within a profile group, for each wireless radio, rate limiting needs to add up to a maximum of 100 percent. (It can be less than 100 percent.)

For example, within one profile group, if four profiles use the 802.11b/bg/ng mode and two profiles use the 802.11a/na mode, you create one rate-limiting configuration for the four profiles that use the 802.11b/bg/ng mode and another rate-limiting configuration for the two profiles that use the 802.11a/na mode. The combined percentages of the four profiles that

use the 802.11b/bg/ng mode cannot exceed 100 percent; similarly, the combined percentages of the two profiles that use the 802.11a/na mode cannot exceed 100 percent.

On each managed access point (or on each radio in a managed *dual-band* access point), the available bandwidth is distributed in the specified percentages among the profiles in a profile group. The percentage that is configured for a single profile is shared among all the clients connected to it.

If you do not want to configure rate limiting for a profile, configure rate limiting as 0 (zero) percent. This effectively disables rate limiting for that profile. A setting of 0 (zero) percent can work well for profiles that are used for management, administration, or testing.

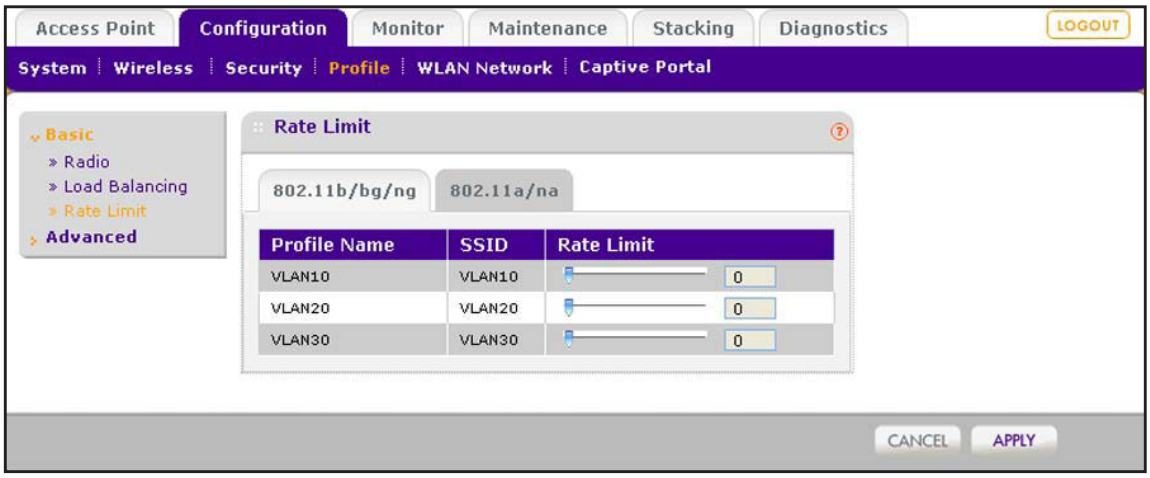
Rate Limiting for the Basic Profile Group

In the basic profile group, for each radio mode (802.11b/bg/ng mode and 802.11a/na mode), rate limiting per profile adds up to a maximum of 100 percent. (It can be less than 100 percent.) There is a tab for each wireless radio mode.

➢ **To configure rate limiting for the basic profile group:**

1. Select **Configuration > Profile > Basic > Rate Limit**.

   The basic Rate Limit screen displays:



2. Click the tab for the radio for which you want to configure rate limiting.
3. For each profile on a wireless radio, specify the rate limit as a percentage.

   You can drag the sliders to adjust the values in the rate limit fields to the right of the sliders. Make sure that the total percentages of all profiles on one wireless radio do not exceed 100 percent.

4. Click **Apply**.

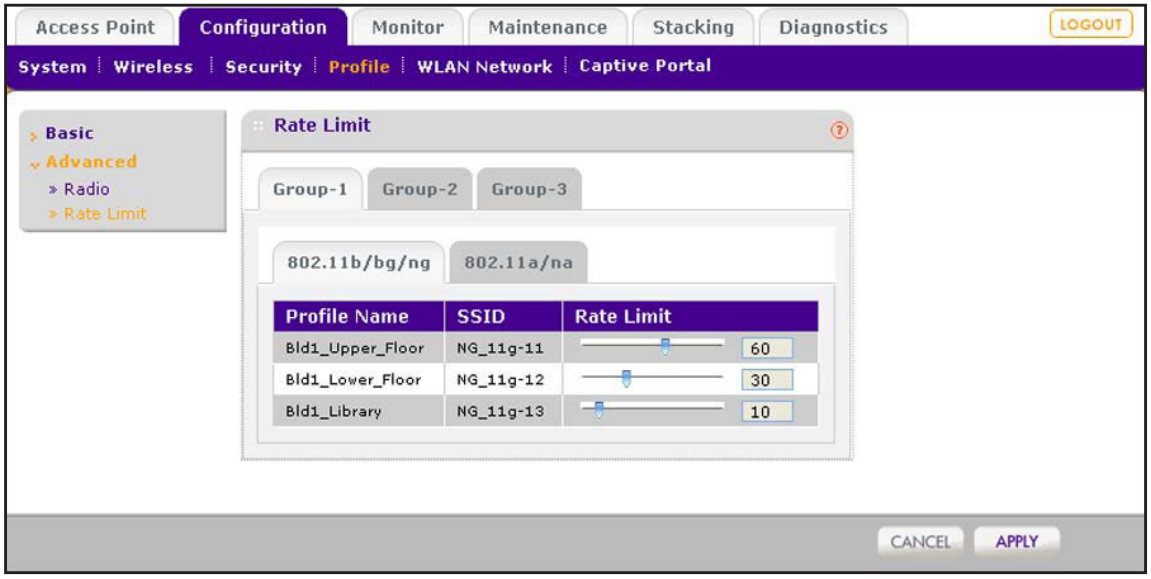
Rate Limiting for an Advanced Profile Group

For each profile group, and for each radio mode (802.11b/bg/ng mode and 802.11a/na mode), rate limiting per profile adds up to a maximum of 100 percent. (It can be less than 100 percent.) There is a tab for each group and for each wireless radio mode.

➢ **To configure rate limiting for an advanced profile group:**

1. Select **Configuration > Profile > Advanced > Rate Limit**.

   The advanced Rate Limit screen displays:



2. Click the tab for the profile group for which you want to configure rate limiting.
3. Click the tab for the radio for which you want to configure rate limiting.
4. For each profile on a wireless radio in the selected profile group, specify the rate limit as a percentage.

   You can drag the sliders to adjust the values in the rate limit fields to the right of the sliders. Make sure that the total percentages of all profiles on one wireless radio in the selected profile group do not exceed 100 percent.

5. Click **Apply**.

Maintain the Wireless Controller and Access Points

9

This chapter includes the following sections:

- *Manage the Configuration File*
- *Reboot or Reset the Wireless Controller*
- *Manage Remote Access*
- *Specify Session Time-Outs*
- *View Alerts and Events and Save the Logs*
- *Manage Licenses*
- *Reboot Access Points*
- *Configure Multicast Firmware Upgrade for Access Points*

Note: Although the web management interface provides an Extended Storage menu tab, extended (or external) storage is not supported. Extended storage will be supported in a future release.

Manage the Configuration File

This section includes the following subsections:

- *Back Up the Configuration File*
- *Restore the Configuration File*
- *Upgrade the Firmware*

The configuration settings of the wireless controller are stored in a configuration file on the wireless controller. This file can be saved (backed up) to a computer, retrieved (restored) from the computer, cleared to factory default settings, and replaced by a newer version (upgraded).

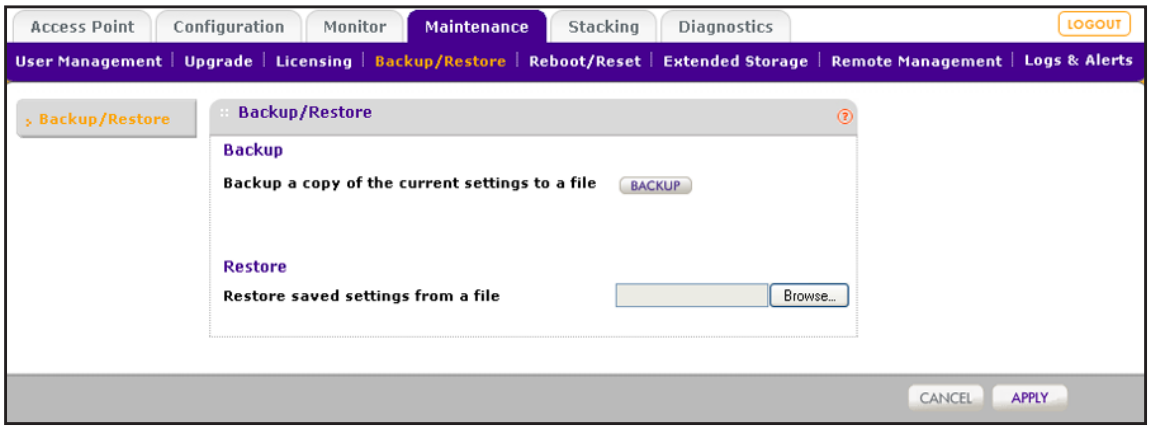
Back Up the Configuration File

Once the wireless controller is installed and works correctly, make a backup of the configuration file to a computer. If necessary, you can later restore the wireless controller settings from this file.

➢ **To back up the configuration file and save a copy of the current settings:**

1. Select **Maintenance > Backup/Restore**.

   The Backup/Restore screen displays:



2. Click the **Backup** button.

   A dialog box displays, showing the file name of the backup file. The backup file has the following format: backup.tar.gz.

3. Follow the instructions of your browser to save the configuration file.

Restore the Configuration File

Restore only settings that were backed up from a WC9500 wireless controller. (You cannot restore settings on a WC9500 wireless controller that were backed up from a WC7520 wireless controller.)

➢ **To restore the configuration file from a backed-up file:**

1. Select **Maintenance > Backup/Restore**.

   The Backup/Restore screen displays.

2. Click the **Browse** button.
3. Navigate to the saved configuration file.

WARNING:

When you click Apply to restore the configuration file, do not try to go online, turn off the wireless controller, shut down the computer, or do anything else to the wireless controller until the wireless controller finishes rebooting. When the Status LED turns green, wait a few more seconds before you do anything.

4. Click **Apply**.

   The configuration file is loaded onto the wireless controller, and the wireless controller reboots.

Upgrade the Firmware

The wireless controller provides two methods for upgrading its firmware:

- Scheduled, automatic update
- Manual update

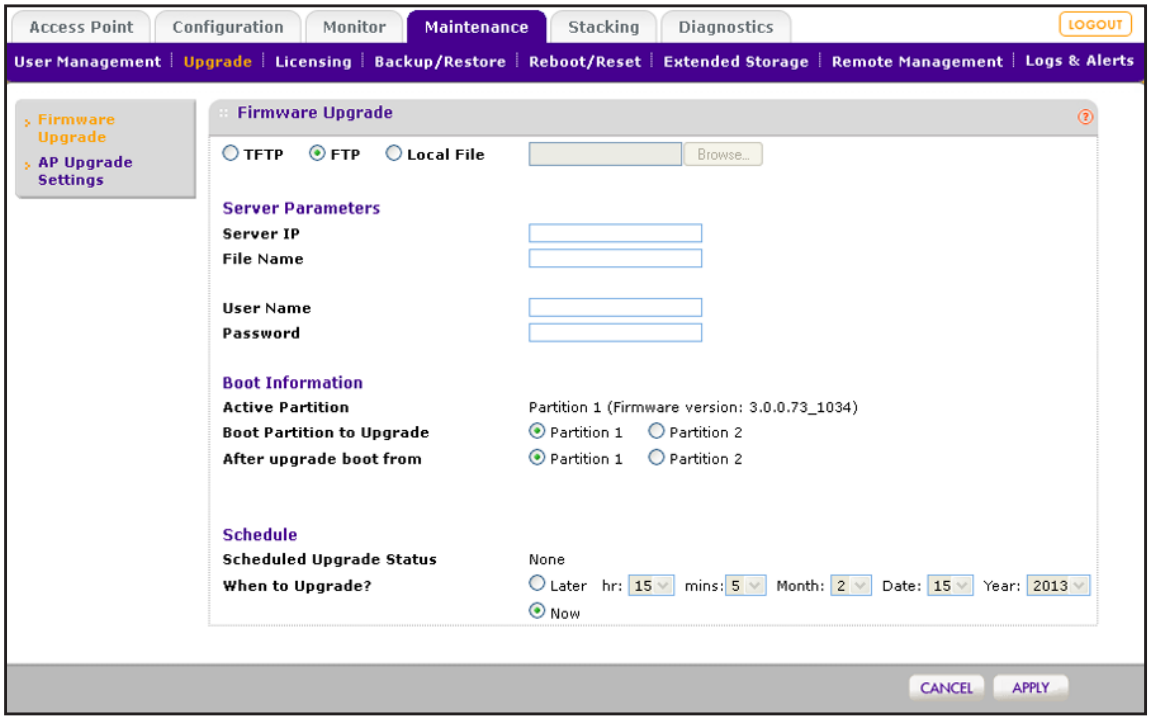
There are two boot partitions to allow you to switch the wireless controller from one firmware version to another. You can configure the wireless controller to download firmware from a TFTP or FTP server and upgrade the firmware on the wireless controller when it is least disruptive. You can also download firmware manually to a computer and upload it to the wireless controller from a local file.

Note: In some cases, such as a major firmware upgrade, you might need to erase the configuration and manually reconfigure the wireless controller after the firmware upgrade. Refer to the Release Notes for the firmware version to find out if you need to reconfigure the wireless controller.

➢ **To upgrade the firmware:**

1. (Optional) Download the firmware from NETGEAR:
   a. Visit the NETGEAR support page for the WC9500 wireless controller at *http://support.netgear.com/product/WC9500*.
   b. Download the firmware and save it to your computer.
2. Select **Maintenance > Upgrade > Firmware Upgrade**.

   The Firmware Upgrade screen displays. The following figure shows the fields that display when you have selected the FTP radio button. When you select the TFTP or Local File radio button, fewer fields are shown.



3. Configure the settings as described in the following table:

Setting	Description
TFTP, FTP, or Local File	Select one of the following radio buttons to specify from which location the upgrade should occur. The screen adjusts to display the fields that are required for each upgrade location. • **TFTP**. Upgrade from a TFTP server. The Server IP and File Name server parameters fields display. • **FTP**. Upgrade from an FTP server. The Server IP, File Name, User Name, and Password server parameters fields display. • **Local File**. Upgrade from a local file that you have downloaded. The server parameter fields do not display, but the Browse field becomes available. Follow the directions of your browser to select the firmware upgrade file from your computer.

Setting	Description
Server Parameters section (TFTP and FTP only)	
Server IP	Enter the IP address of the TFTP or FTP server.
File Name	Enter the file name of the firmware.
User Name (FTP only)	Enter the user name to access the FTP server.
Password (FTP only)	Enter the password to access the FTP server.
Boot Information section	
Active Partition	This is an informational field that displays the active partition and the current firmware version.
Boot Partition to Upgrade	Select the radio button for the partition to which the new firmware should be saved.
After upgrade boot from	Select the radio button for the partition from which the wireless controller should reboot after the firmware has been upgraded.
Schedule section	
Schedule Update Status	This is an informational field that displays when the firmware upgrade will occur. If no update is scheduled, the field displays None.
When to Upgrade?	Select when the firmware upgrade should occur: • **Later**. Make selections from the menus to specify the date and time when the upgrade should occur. • **Now**. The upgrade occurs immediately after you click Apply.

WARNING:

When you click Apply and the Now radio button is selected to upgrade the firmware immediately, do not try to go online, turn off the wireless controller, shut down the computer, or do anything else to the wireless controller until the wireless controller finishes rebooting. When the Status LED turns green, wait a few more seconds before you do anything.

4. Click **Apply**.

   Unless you scheduled the firmware upgrade for a particular time, the firmware is upgraded immediately, and the wireless controller reboots.

5. (Optional) Verify that the wireless controller is running the latest firmware:
   a. Select **Monitor > Network > Controller**.

      The Controllers screen displays.

   b. Verify the firmware version in the Version column.

Note: After you have upgraded the firmware, if the browser does not display the latest features of the web management interface, clear the browser's cache, and refresh the screen.

Reboot or Reset the Wireless Controller

The Reboot/Reset Controllers screen lets you reboot or reset the wireless controller.

There are two types of reset:

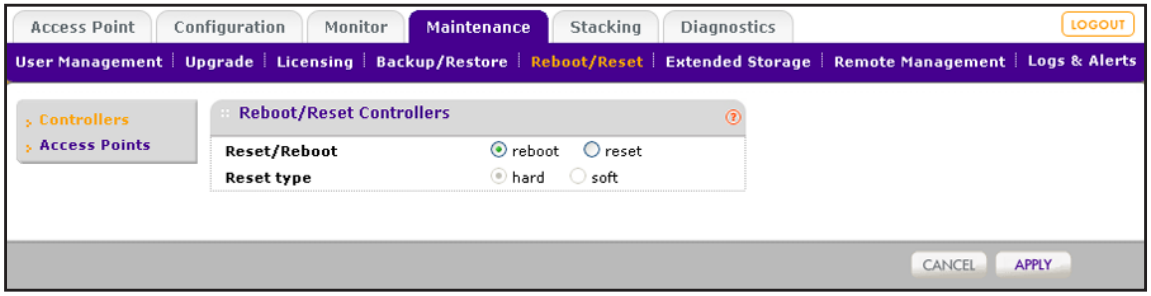
- **Hard reset**. The settings of the wireless controller are restored to factory default settings. This reset has the same function as the Reset button on the front panel.
- **Soft reset**. Saves the IP and VLAN addresses and managed access point list but clears all other settings such as profiles, profile groups, and authentication servers.

Note: Restoring the factory default settings of the wireless controller does *not* restore the settings of the access points that are managed by the wireless controller.

➢ **To reboot the wireless controller:**

1. Select **Maintenance > Reboot/Reset > Controllers**.

   The Reboot/Reset Controllers screen displays:



2. Select the **reboot** radio button.
3. Click **Apply**.

   The wireless controller reboots. The reboot process is complete after several minutes when the Status LED on the front panel turns green.

➢ **To reset the wireless controller:**

1. Select **Maintenance > Reboot/Reset > Controllers**.

   The Reboot/Reset Controllers screen displays.

2. Select the **reset** radio button.
3. Select one of the following radio buttons to specify a hard reset or soft reset:
   - **hard**. Restore the factory default settings to the wireless controller. The factory default settings are listed in *Appendix A, Factory Default Settings and Technical Specifications*.
   - **soft**. Clear all settings except for the IP and VLAN addresses and managed access point list.

WARNING:

When you have selected the hard radio button and you click Apply, do not try to go online, turn off the wireless controller, shut down the computer, or do anything else to the wireless controller until the wireless controller finishes rebooting. When the Status LED turns green, wait a few more seconds before you do anything.

4. Click **Apply**.

   The configuration file is restored according to the selection that you made, and the wireless controller reboots.

Manage Remote Access

Enable SNMP to allow SNMP network management software, such as HP OpenView, to monitor the wireless controller by using SNMPv1 or SNMPv2c protocol.

You can configure the wireless controller through SNMP, except for the following features:

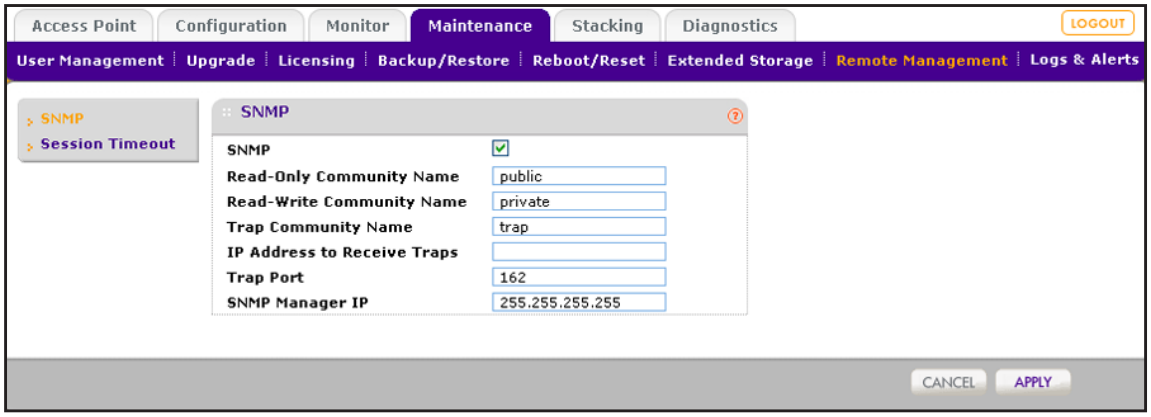
- Guest access management
- RF management

Note: The wireless controller supports SSH through the console port. However, the console port is for debugging under guidance of NETGEAR technical support only.

➢ **To enable and configure SNMP:**

1. Select **Maintenance > Remote Management > SNMP**.

   The SNMP screen displays:



2. Enable SNMP and configure the settings as described in the following table:

Setting	Description
SNMP	Select this check box to enable SNMP for the wireless controller.
Read-Only Community Name	Enter the community string that allows the SNMP manager to read the wireless controller's MIB objects. The default setting is public.
Read-Write Community Name	Enter the community string that allows the SNMP manager to read and write the wireless controller's MIB objects. The default setting is private.
Trap Community Name	Enter the community name that is associated with the IP address to receive traps. The default setting is trap.
IP Address to Receive Traps	Enter the IP address at which the SNMP manager receives traps sent from the wireless controller.
Trap Port	Enter the port on which the SNMP manager receives traps sent from the wireless controller. The default setting is port 162.
SNMP Manager IP	Enter the IP address of the SNMP manager. To allow any SNMP manager to access the wireless controller, keep this field blank.

3. Click **Apply**.

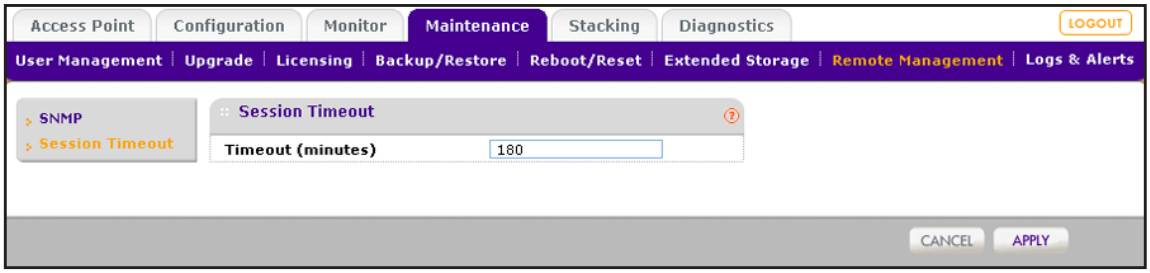
Specify Session Time-Outs

If an HTTP session times out, the user is redirected to the login screen for password verification.

➢ **To specify the length of the HTTP session time-out for the wireless controller:**

1. Select **Maintenance > Remote Management > Session Timeout**.

   The Session Timeout screen displays:



2. In the Timeout (minutes) field, specify number of minutes before an active HTTP login session expires.

   The default session time-out is five minutes.

3. Click **Apply**.

View Alerts and Events and Save the Logs

You can view the system alerts and save the system logs that are collected on the wireless controller. You can also query the system logs for individual access points, clients, and SSIDs. If a problem or failure occurs, these system logs along with backed-up configuration settings could help determine the cause.

NETGEAR recommends that you save the system logs before you clear them.

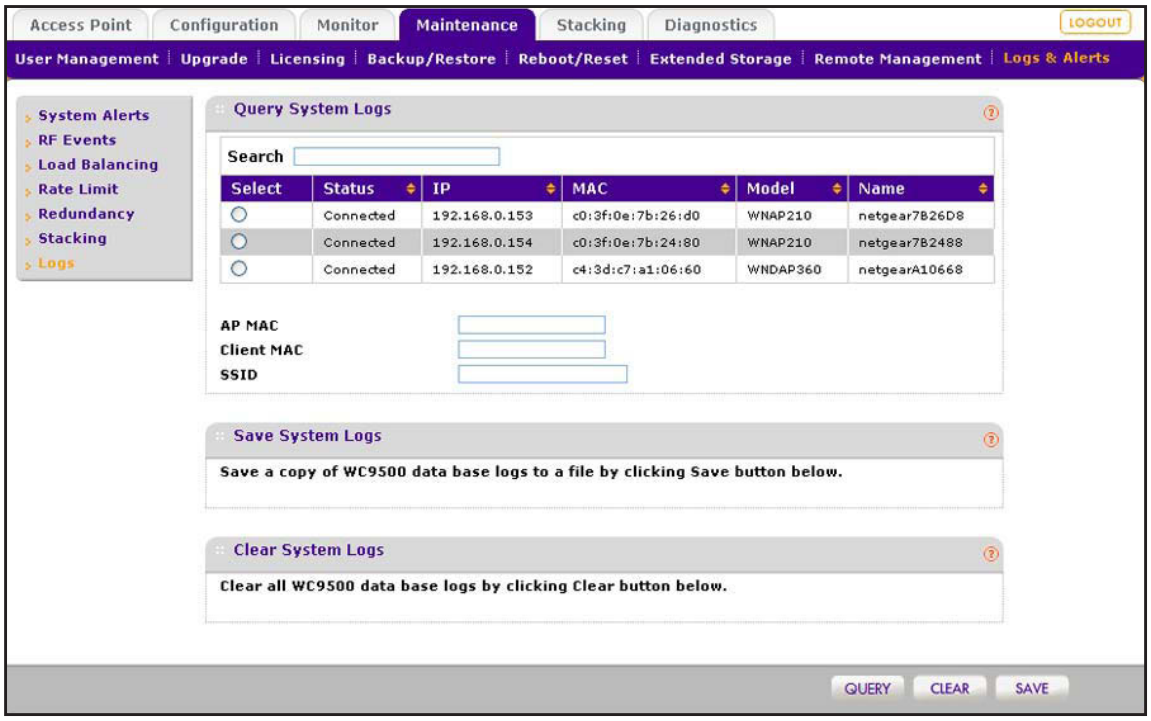
Query the System Logs

The information that is stored in the system logs and that you can query depends on the log settings. For information about how to configure which information is recorded and stored in the logs, see *Configure Log Settings* on page 58.

➢ **To query the system logs for an access point, client, or SSID:**

1. Select **Maintenance > Logs & Alerts > Logs**.

The Query System Logs screen displays:

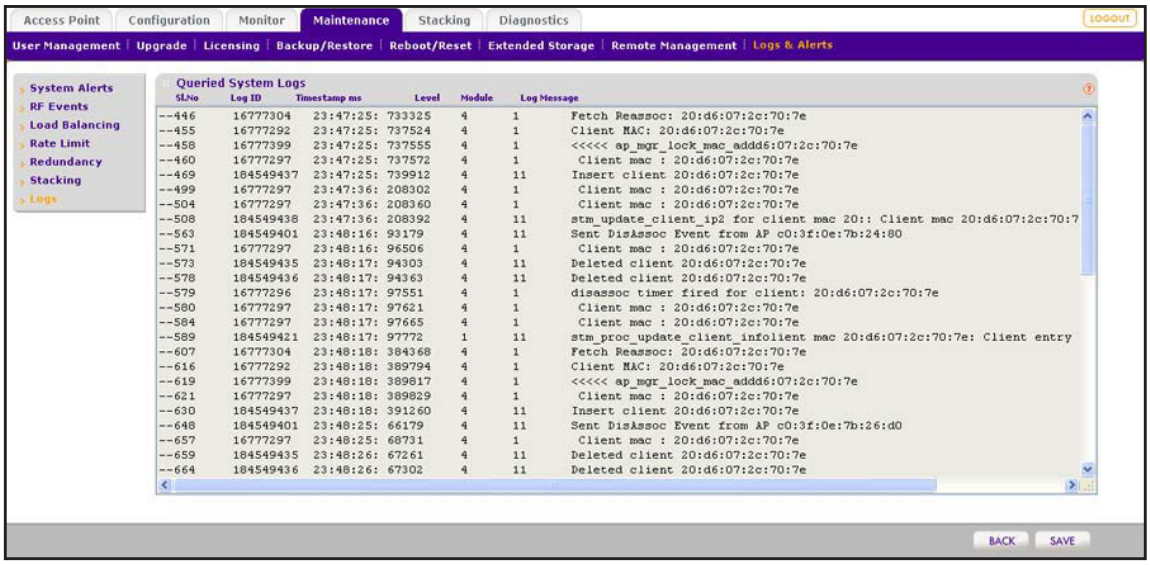


2. (Optional) In the Search field, enter the status (for example, Connected or Disconnected), IP address, MAC address, model, or name of an access point for which you want to query the logs.

   The table displays only the access point or access points that match the information that you entered in the Search field.

3. Take one of the following actions (you can perform *one* query at a time):
   - In the table, select the radio button for the access point for which you want to query the logs.
   - In the IP MAC field, enter the MAC address of the access point for which you want to query the logs.
   - In the Client MAC field, enter the MAC address of the wireless client for which you want to query the logs.
   - In the SSID field, enter the name of the SSID for which you want to query the logs.
4. Click **Query**.

If any logs are available, they are displayed onscreen:



5. (Optional) Click **Save**.
6. Follow the directions of your browser to save the logs to your computer.

   The default name of the zipped log file is <*IP address*>-WC9500-Query.txt, in which <*IP address*> is the IP address of the wireless controller.

7. Click **Back**.

   The Query System Logs screen displays again.

- **To save *all* system logs:**

1. Select **Maintenance > Logs & Alerts > Logs**.

   The Query System Logs screen displays.

2. Click **Save**.
3. Follow the directions of your browser to save the logs to your computer.

   The default name of the zipped log file is <*IP address*>-WC9500-Logs.tgz, in which <*IP address*> is the IP address of the wireless controller.

- **To clear the system logs:**

1. Select **Maintenance > Logs & Alerts > Logs**.

   The Query System Logs screen displays.

2. Click **Clear**.

View Alerts and Events

The wireless controller lets you view the following alerts and events:

- **System alerts**. System alerts such as an access point coming up or being shut down, the wireless controller coming up or being shut down, and a firmware upgrade.
- **RF events**. Radio frequency events such as the detection of a coverage hole, a change of channel, or a managed access point going down.
- **Load balancing** event. Load-balancing events such as a bad RSSI for a client, or the violation of a load-balancing threshold.
- **Rate limiting** events. Rate-limit events such as the violation of a rate-limit threshold.

Note: *The Logs & Alerts menu includes Redundancy and Stacking links. Redundancy and stacking will be supported in a future release.*

Common Components on the Alerts and Events Screens

Each screen that displays alerts or events contains a table with three columns:

- **Severity**. The alarm severity level: All, Minor, Normal, Major, or Critical. You can sort the table on severity level by clicking the icon next to the Severity header in the table.
- **Description**. The description of the alert or event, which is self-explanatory. You can sort the table on description by clicking the icon next to the Description header in the table.
- **Raised Time**. The date and time that the alert or event was raised. You can sort the table on time by clicking the icon next to the Raised Time header in the table.

A table can extend over multiple pages.

The progress bar ( ) shows only when many components (such as access points or clients) are retrieved and require two or more pages to be displayed.

You can navigate through a table by using the following links and menu that display at the bottom of the table only if there are sufficient entries in the table:

- To move to the next page, click **Next**.
- To move to the previous page, click **Previous**.
- To change the number of entries onscreen, select **20**, **40**, **60**, **80**, or **All** from the Entry Per Page menu.

Each screen lets you refresh the alerts or events, export the alerts or events, and clear the alerts or events from the screen and from the memory:

- To display the latest alerts or events onscreen, click **Refresh**.
- To clear all alerts or events from the screen and from memory, click **Clear All**.

  NETGEAR recommends that you save the logs or alerts before you clear them.
- To save the alerts or events:

  a. Click **Export**.

  b. Follow the directions of your browser to save the alerts or events to your computer.

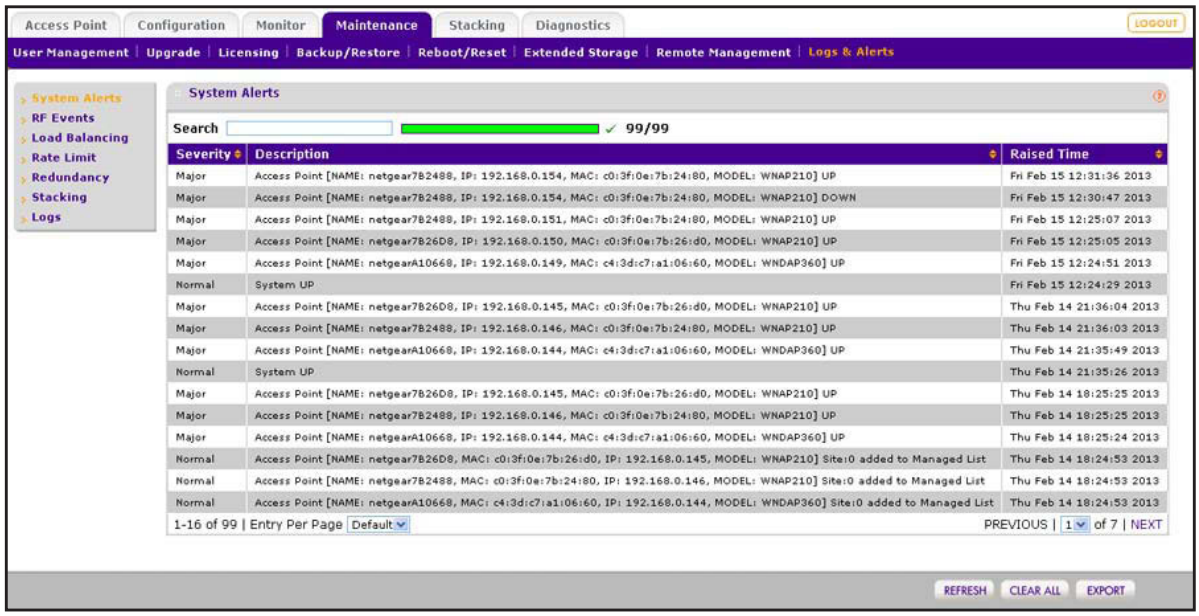
View the Alerts and Events Screens

There are separate screens to view the system alerts, RF events, load-balancing events, and rate-limit events.

➢ **To view system alerts:**

Select **Maintenance > Logs & Alerts > System Alerts**.

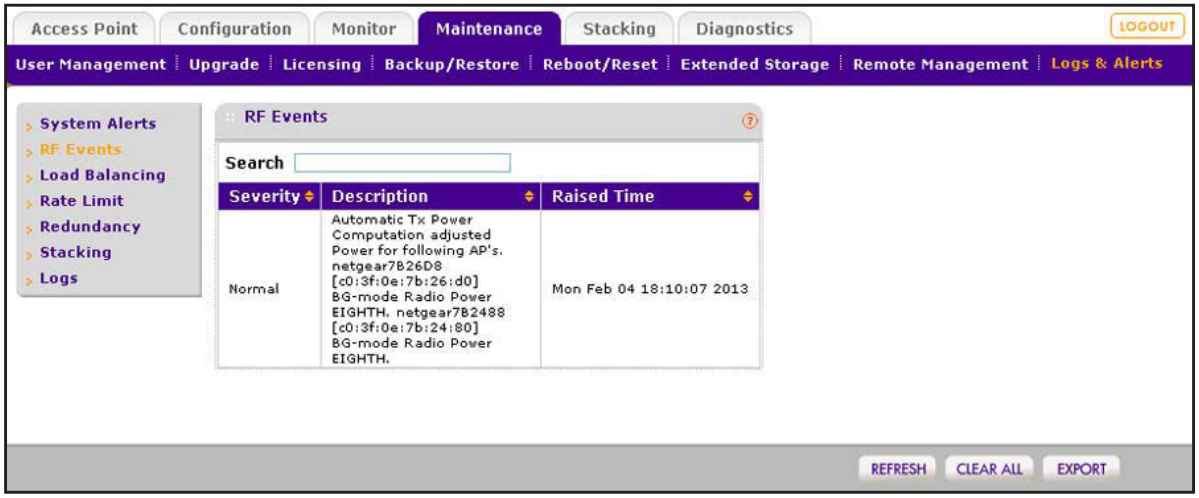
The System Alerts screen displays:



- **To view RF events:**

  Select **Maintenance > Logs & Alerts > RF Events**.

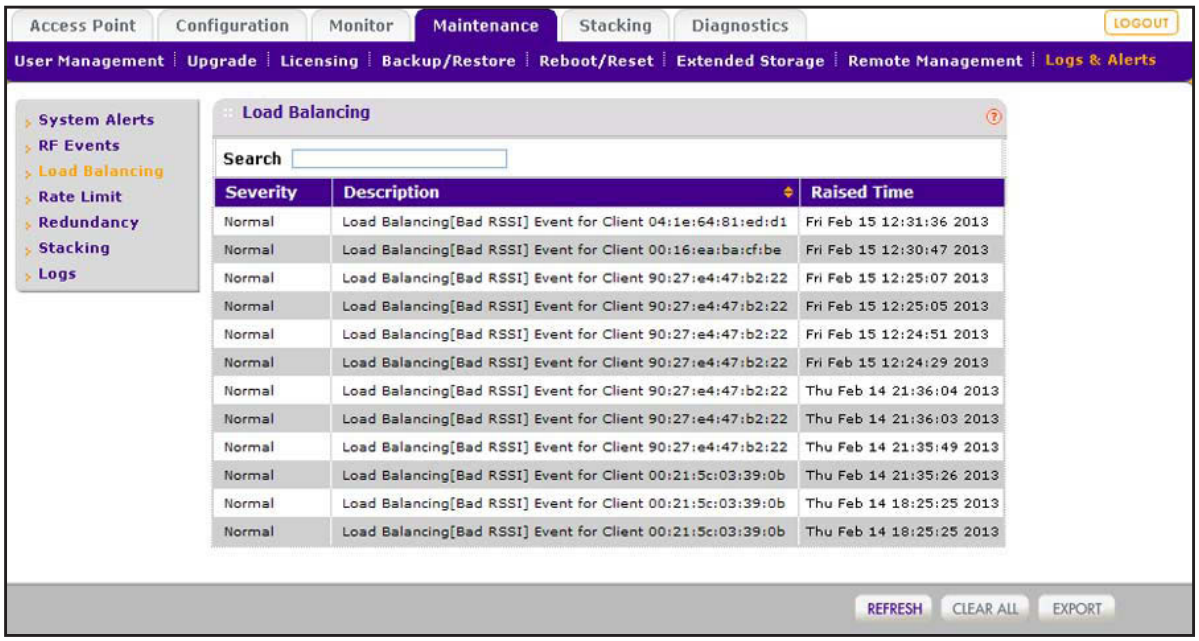
  The RF Events screen displays:



- **To view load-balancing events:**

  Select **Maintenance > Logs & Alerts > Load Balancing**.

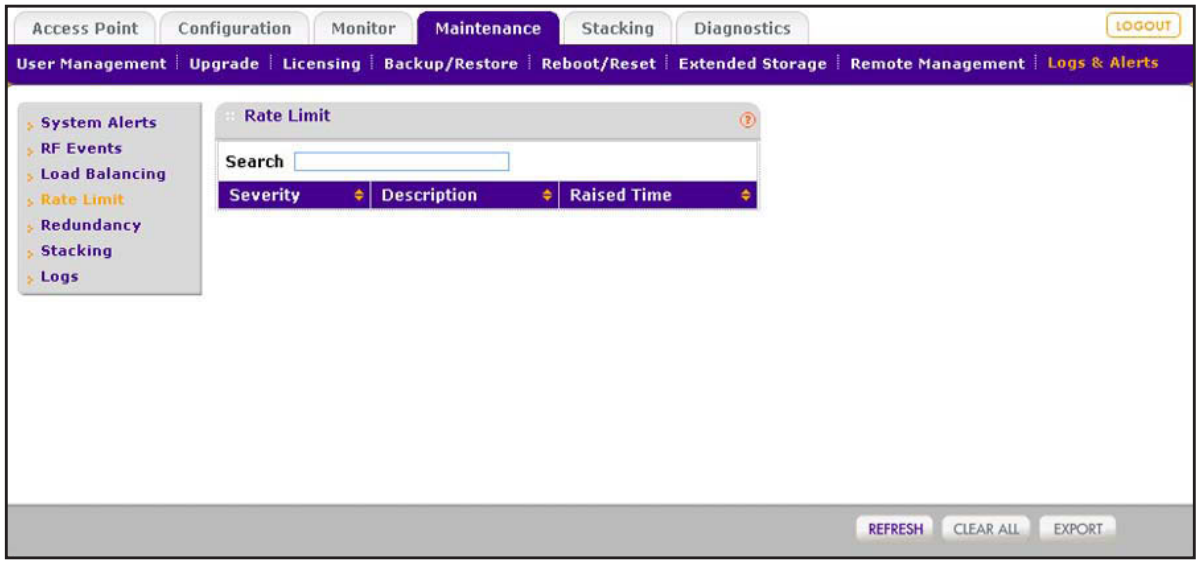
  The Load Balancing screen displays:



➢ **To view rate-limit events:**

Select **Maintenance > Logs & Alerts > Rate Limit**.

The Rate Limit screen displays:



Manage Licenses

The License screen allows you to import, register, and view the licenses that you require for your network. For more information about licenses, see *Licenses* on page 18.

The License screen consists of four separate screens:

- **Inventory**. Provides an overview of your licenses. For information, see *View Your Licenses* on page 165.
- **Server Settings**. Allows you to configure the server settings to import your licenses. For information, see *Configure the License Server Settings* on page 54.
- **Registration**. Allows you to register your licenses. For information, see *Register Your Licenses with the License Server* on page 55.
- **Advanced**. Lets you retrieve your licenses. This screen displays relevant information only if you have received a replacement unit from NETGEAR. Under normal circumstances, you do not need this screen. For information, see *Retrieve Your Licenses* on page 167.

View Your Licenses

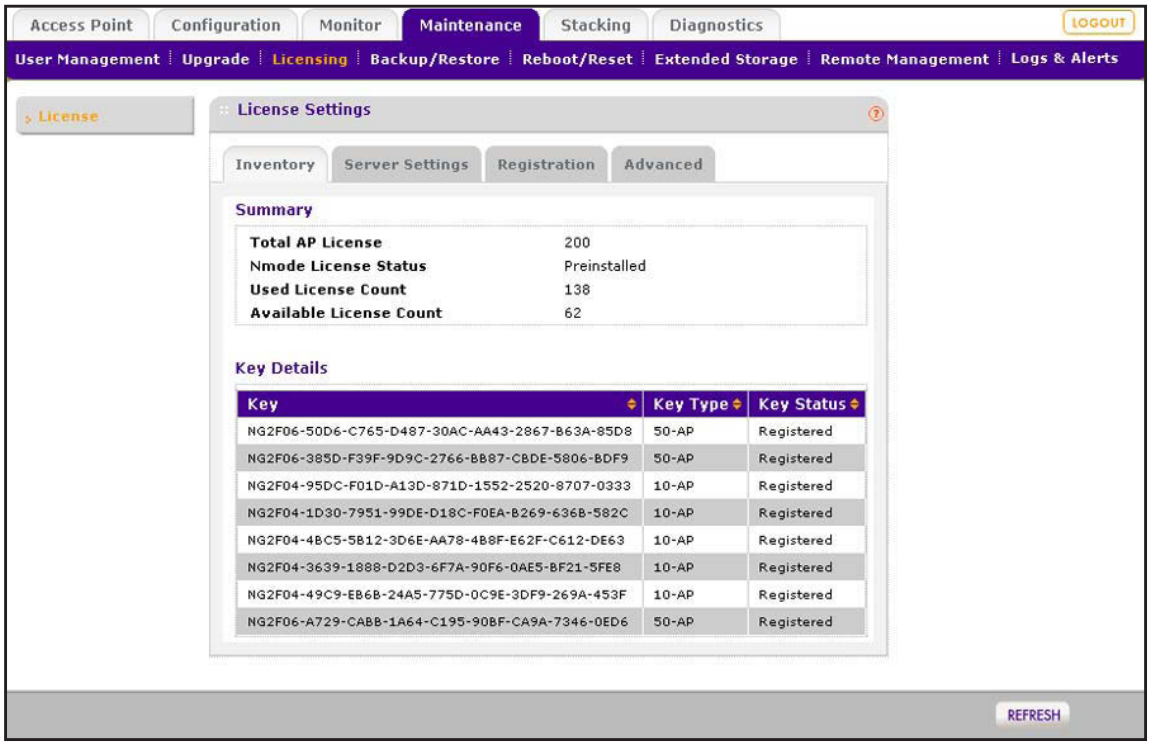
When your licenses are installed and registered, you can view them on the Inventory screen.

➢ **To view your licenses:**

1. Select **Maintenance > License**.

2. Click the **Inventory** tab.

   The Inventory screen displays:



   The following table describes the fields of the screen:

Setting	Description
Summary section	
Total AP License	The number of access points that your licenses support.
Nmode License Status	Availability of the 802.11n mode license. (This license is available by default, indicated by either Pre-installed or Available.)
Used License Count	The number of access points that are used from the total number that your licenses support.
Available License Count	The number of access points that are still available from the total number that your licenses support.
Key Details section	
Key	The value of the key that unlocks the license.
Key Type	The type of the key that determines the number of access points that are supported and the mode that is supported.
Key Status	The status of the key (Registering key with server or Registered).

3. (Optional) Click **Refresh**.

Your license information is refreshed onscreen.

Retrieve Your Licenses

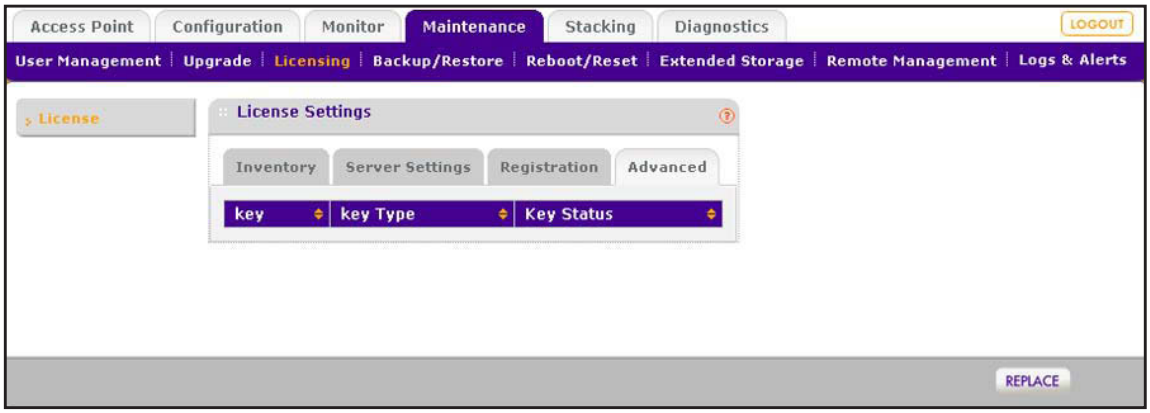
If NETGEAR exchanged your wireless controller for another one, your licenses no longer display on the Inventory and Registration screens. You need to retrieve your licenses from the license update server.

➢ **To retrieve licenses after you have received a replacement unit from NETGEAR:**

1. Make sure that the wireless controller is connected to the Internet.
2. Make sure that the DNS servers are configured correctly.

   For information about configuring DNS servers, see *IP and VLAN Settings* on page 49.
3. Select **Maintenance > License**.
4. Click the **Advanced** tab.

   The Advanced screen displays.



5. Click **Replace**.

   The wireless controller connects to the license update server and retrieves your licenses.

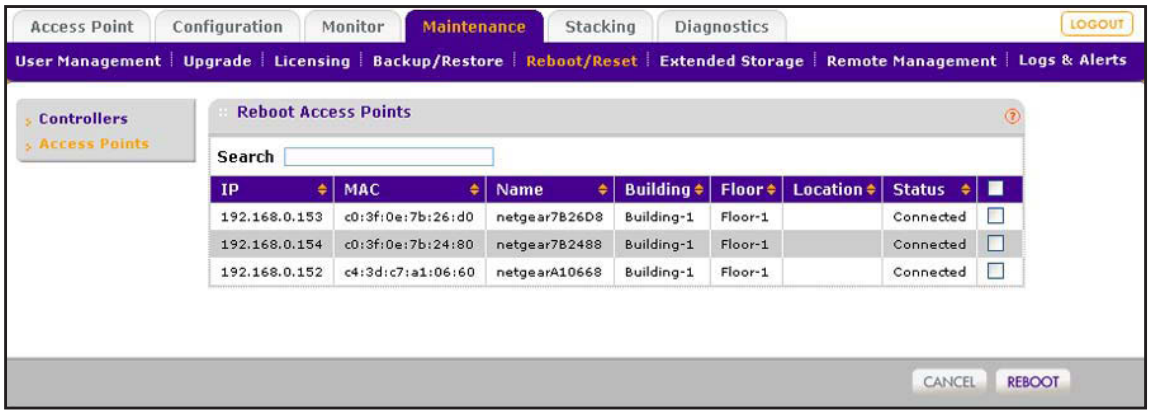
Reboot Access Points

Under normal circumstances, there is no reason to reboot an access point. If there is a problem with an access point, you can reboot it to see if this resolves the problem.

➢ **To reboot an access point:**

1. Select **Maintenance > Reboot/Reset > Access Points**.

The Reboot Access Points screen displays:



2. (Optional) In the Search field, enter the IP address, MAC address, model, or name of an access point that you want to reboot, or enter other information to narrow down the information that is displayed in the table.

   The table displays only the access point or access points that match the information that you entered in the Search field.

3. Take one of the following actions:
   - Select a single access point by selecting the check box to the right of the access point.
   - Make a selection of access points by selecting the check boxes to the right of the access points.
   - Select all access points by selecting the check box in the upper right of the table heading.

4. Click **Reboot**.

   The selected access point or access points are rebooted.

Configure Multicast Firmware Upgrade for Access Points

When you add access points to the managed list (see *Chapter 6, Discover and Manage Access Points*), the wireless controller upgrades the firmware of the access points to the latest firmware that is loaded on the wireless controller. By default, this firmware upgrade process uses multicast, which allows all access points to be upgraded simultaneously. If you need to, you can disable multicast and let the wireless controller use unicast for the firmware upgrade process (see *Disable Multicast Firmware Upgrade* on page 169). Also, if the multicast firmware upgrade process fails three times, the wireless controller automatically switches to the unicast firmware upgrade process.

With the default multicast firmware upgrade process, the wireless controller distributes multicast IP addresses to the access points, enabling them to join the multicast group and to receive the firmware upgrade.

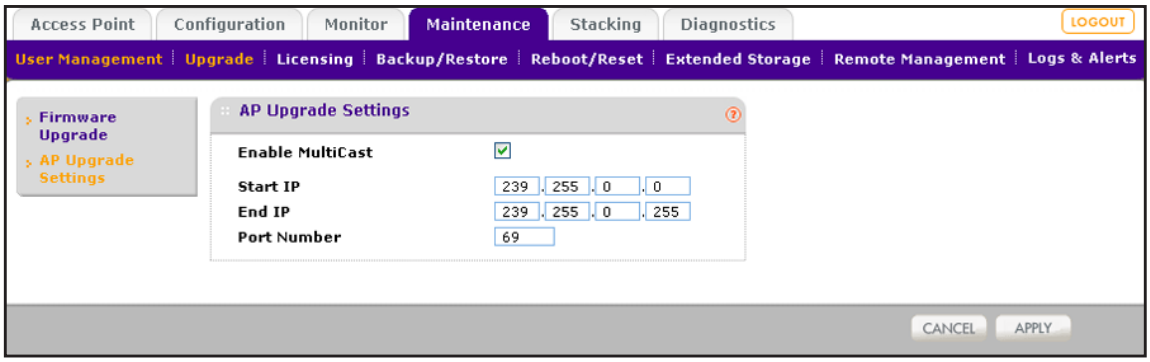
Change the Multicast Firmware Upgrade Settings

By default, the wireless controller uses IP range 239.255.0.0–239.255.0.255 for the multicast firmware upgrade process. If your network requires that the wireless controller uses a different multicast IP range, you can configure the IP range on the AP Upgrade Settings screen.

➢ **To configure another multicast IP address range and port for the firmware upgrade process:**

1. Select **Maintenance > Upgrade > AP Upgrade Settings**.

   The AP Upgrade Settings screen displays.



2. Configure the settings as described in the following table

Setting	Description
Start IP	Enter the start IP address of the multicast range that the wireless controller should use.
End IP	Enter the end IP address of the multicast range that the wireless controller should use.
Port Number	Enter the port number that the wireless controller should use. The default number is 69.

3. Click **Apply**.

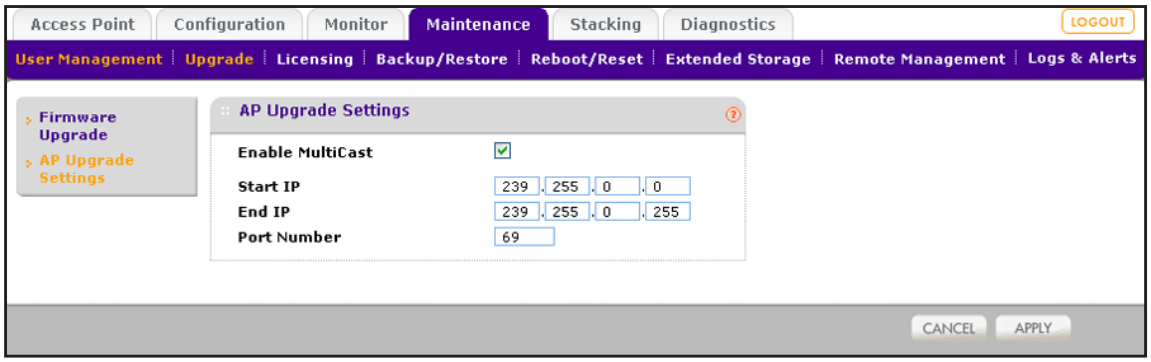
Disable Multicast Firmware Upgrade

There might be network configurations in which you cannot use multicast. If you disable multicast on the AP Upgrade Setting screen, the firmware upgrade process uses unicast, which is a slower process because the firmware upgrade is applied to groups of access points instead of simultaneously to all access points. The time that the unicast firmware upgrade process takes depends on the network load and on the type of Ethernet interface to which the wireless controller is connected.

➢ **To disable multicast firmware upgrade for access points:**

1. Select **Maintenance > Upgrade > AP Upgrade Settings**.

The AP Upgrade Settings screen displays.



2. Clear the **Enable Multicast** check box.

   This check box is selected by default.

3. Click **Apply**.

Monitor the Wireless Network and Its Components

10

This chapter includes the following sections:

- *Common Tasks on the Monitoring Screens*
- *Monitor the Wireless Controller*
- *Monitor the SSIDs*
- *Monitor Local Clients*

Note: The information that is shown in the figures in this chapter is not always consistent. That is, the information in one figure might be for a different network configuration than the information in another figure.

Common Tasks on the Monitoring Screens

The monitoring screens display *read-only* status information of the network that is managed by the wireless controller. The following sections describe common tasks that you can perform on many monitoring screens.

Sort a Table

You can sort a table on any column header that has a double triangle icon or single triangle icon placed to the right of it.

➢ **To sort a table:**

Click a double triangle icon or single triangle icon next to a column header.

Search a Table

Most monitoring screens provide a Search field that lets you search a table on any information that is listed in the table.

➢ **To search a table:**

In the Search field, enter the information that you are looking for such as an IP address, MAC address, name, or anything else.

(There is no Search button to click.)

Navigate through a Table

Tables on the monitoring screens can extend over multiple pages.

The progress bar ( ) shows only when many components (such as access points or clients) are retrieved and require two or more pages to be displayed.

You can navigate through a table by using the following links and menu that display at the bottom of the table only if there are sufficient entries in the table:

➢ **To navigate through a table:**

- To move to the next page, click **Next**.
- To move to the previous page, click **Previous**.
- To change the number of entries onscreen, select **20**, **40**, **60**, **80**, or **All** from the Entry Per Page menu.

Use the Buttons to Perform Specific Tasks

Most screens let you refresh the information and some screens let you clear the information onscreen or export the information:

- To display the latest information onscreen, click **Refresh**.
- To clear the information that is displayed onscreen, click **Clear All**.

- To save the information that is shown onscreen:
  a. Click **Export**.
  b. Follow the directions of your browser to save the alerts or events to your computer.

Note: *The Location button that is shown on some screens is not functional in this release. The location functionality will be added in a later release.*

Monitor the Wireless Controller

You can view a summary of the status of the wireless controller and its components and view individual components:

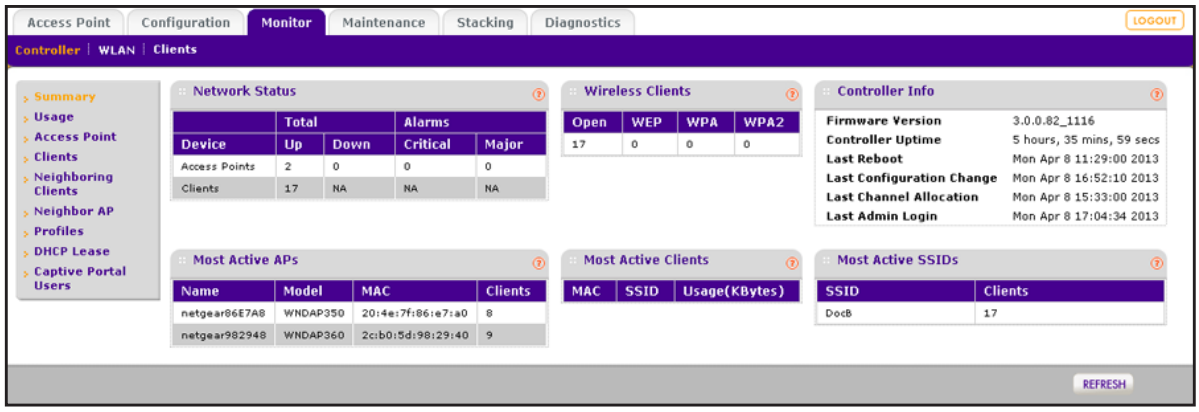
- **Summary**. See *View the Wireless Controller Summary Screen*.
- **Usage**. See *View Wireless Controller Usage*.
- **Access Points**. See *View Access Points Managed by the Wireless Controller*.
- **Clients**. See *View Clients Managed by the Wireless Controller*.
- **Neighboring Clients**. See *View Neighboring Clients Detected by the Wireless Controller*.
- **Neighboring APs**. See *View Neighboring Access Points Detected by the Wireless Controller*.
- **Profiles**. See *View Security Profiles Managed by the Wireless Controller*.
- **DHCP Lease**. See *View DHCP Leases Provided by the Wireless Controller*.
- **Captive Portal Users**. See *View Captive Portal Users Managed by the Wireless Controller*.

View the Wireless Controller Summary Screen

The Summary screen provides an overview of the activity on the wireless controller. When you log in to the web management interface, the Summary screen displays.

➢ **To view the Summary screen:**

Select **Monitor > Controller > Summary**.



The following table describes the fields of the Network Status, Wireless Clients, Most Active APs, Most Active Clients and Most Active SSIDs tables of the screen. The Controller Info section is self-explanatory.

Item		Description
Network Status		
Total	Up	The total number of managed devices that are running correctly.
	Down	The total number of managed devices that cannot be pinged.
Alarms	Critical	The wireless controller can ping these managed devices, but either cannot log in or has detected that these devices are different from the ones that were configured.
	Major	The number of managed devices for which the configuration differs from the one that is set on the wireless controller. This situation occurs most likely because the device runs outdated firmware or the wireless controller changed the configuration while the device was down or offline.
Wireless Clients		
Open		The number of wireless clients that are connected to managed access points using security profiles configured with open mode.
WEP		The number of wireless clients that are connected to managed access points using security profiles configured with WEP.
WPA		The number of wireless clients that are connected to managed access points using security profiles configured with WPA.
WPA2		The number of wireless clients that are connected to managed access points using security profiles configured with WPA2.
Most Active APs For the most active access points, the following information displays:		
Name		The name of the access point (see *Edit Access Point Information on the Managed AP List* on page 101).
Model		The model of the access point (WNAP210, WNAP320, WNDAP350, WNDAP360, or WNDAP380R).
MAC		The MAC address of the access point.
Clients		The number of clients that are associated with the access point.
Most Active Clients For the most active clients, the following information displays:		
MAC		The MAC address of the wireless client.
SSID		The wireless network SSID that the wireless client is using to connect to the access point.
Usage (KBytes)		The traffic usage of the wireless client in KB.

Item	Description
Most Active SSIDs For the most active SSIDs, the following information displays:	
SSID	The name of the wireless network SSID.
Clients	The number of clients that are using the SSID.

View Wireless Controller Usage

The screen displays graphics that show the access point usage, SSID usage, and number of clients on the wireless controller.

Note: Adobe Flash player 10 or later is required to display the graphics.

➢ **To view the Usage screen:**

Select **Monitor > Controller > Usage**.

Data for the 2.4 GHz network (for the combined 802.11b-, 802.11bg-, and 802.11ng-modes) is shown in purple; data for the 5 GHz network (for the combined 802.11a- and 802.11na-modes) is shown in green. The screen shows the following graphs:

- **AP Usage**. Displays the 2.4 GHz and 5 GHz traffic usage in MB for access points.
- **SSID Usage**. Displays the 2.4 GHz and 5 GHz traffic usage in MB for SSIDs.
- **Number of Clients**. Displays the total number of clients, number of clients in the 2.4 GHz network, and number of clients in the 5 GHz network over a period.

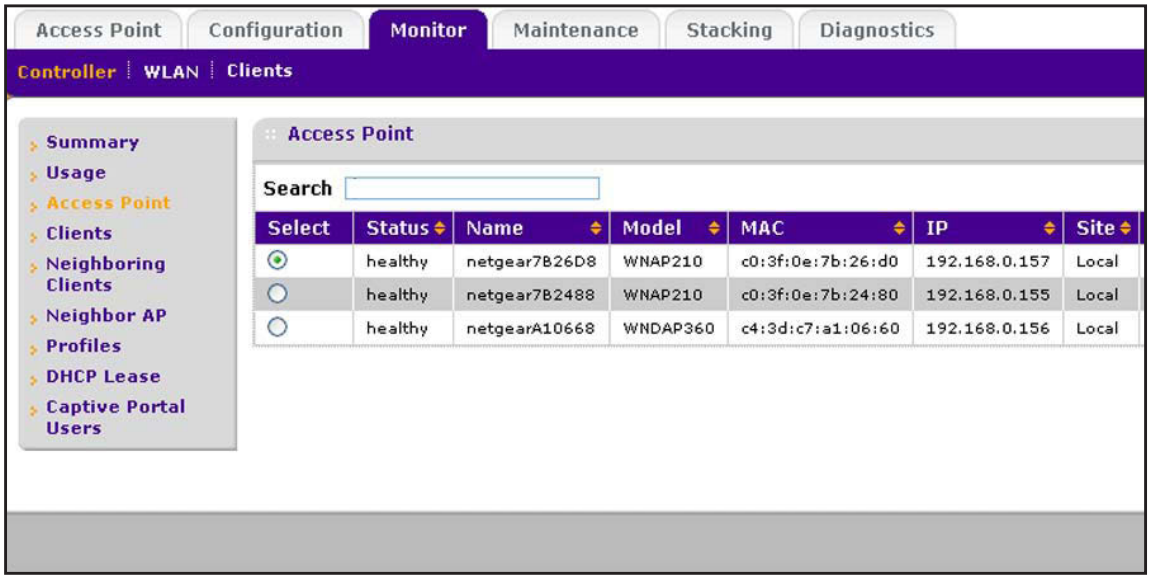
View Access Points Managed by the Wireless Controller

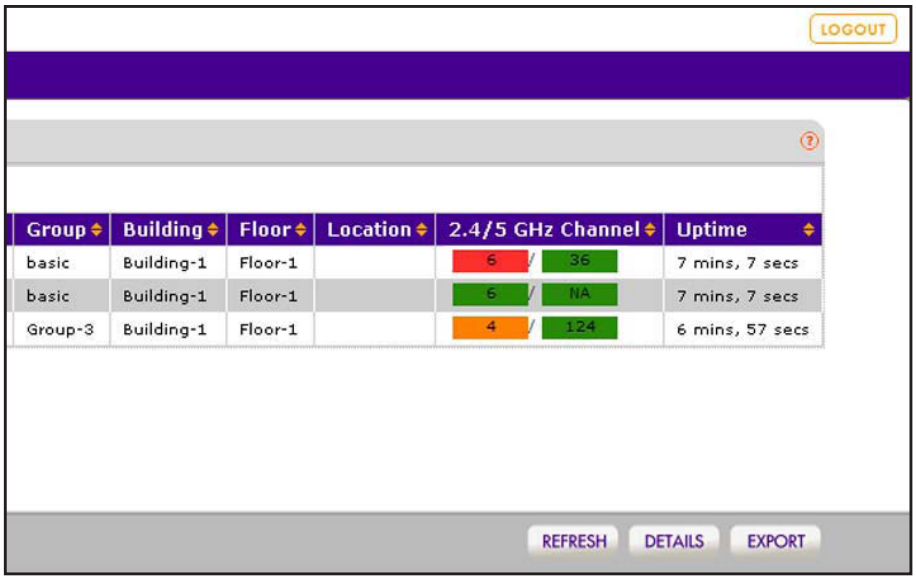
The Access Point screen lets you monitor all access points that are managed by the wireless controller.

➢ **To view the Access Point screen:**

1. Select **Monitor > Controller > Access Point**.

   Because this screen is a wide screen, it is shown in the following two figures:





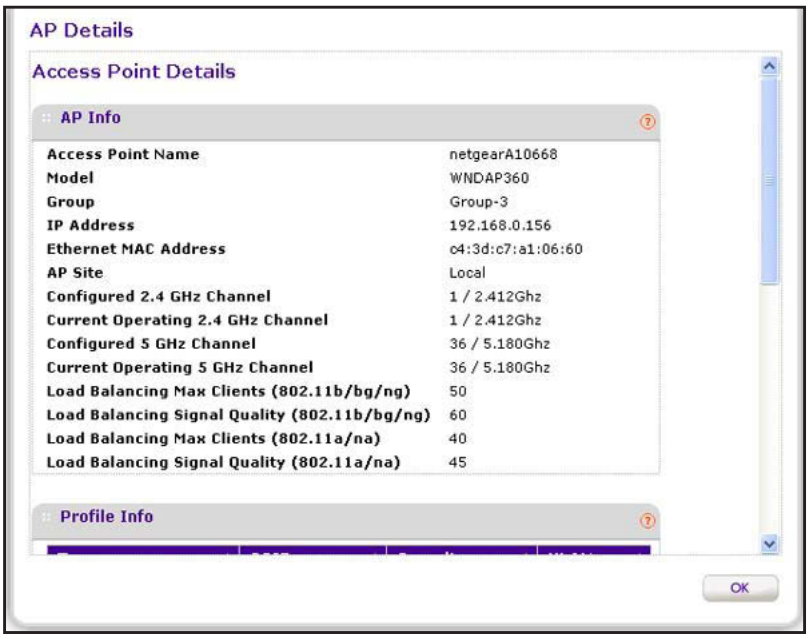
The following table describes the fields of the Access Point table:

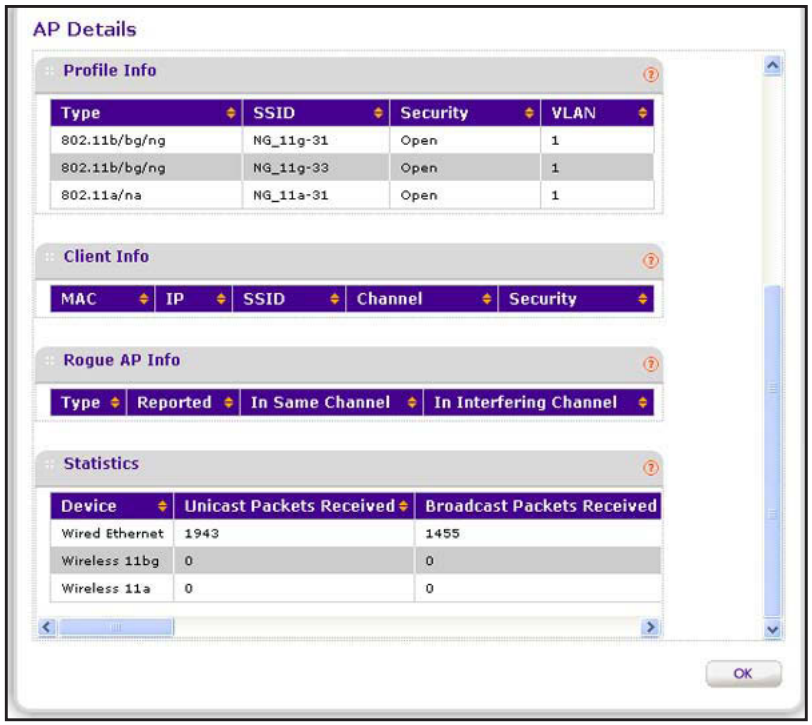
Item	Description
Select	The radio button that lets you select the access point.
Status	The status of the access point (healthy or down).
Name	The name of the access point (see *Edit Access Point Information on the Managed AP List* on page 101).
Model	The model of the access point (WNAP210, WNAP320, WNDAP350, WNDAP360, or WNDAP380R).
MAC	The MAC address of the access point.
IP	The IP address of the access point.
Site	The site designation is always Local.
Group	The profile group to which the access point is assigned (see *Assign Access Points to Advanced Profile Groups* on page 104).
Building	The building designation is always Building-1.
Floor	The floor designation is always Floor-1.
Location	The location of the access point (see *Edit Access Point Information on the Managed AP List* on page 101).

Item	Description
2.4/5 GHz Channel	The active 2.4 GHz or 5 GHz channel on the access point. This information can change after initial configuration of the access point because of automatic channel allocation. The color coding specifies the channel utilization on each radio and has the following meaning: • **Green**. 0–40 percent utilization. • **Light green**. 41–60 percent utilization. • **Orange**. 61–80 percent utilization. • **Red**. 81–100 percent utilization. • **NA**. The radio does not support the band.
Uptime	The period since the access point was last restarted.

2. (Optional) To see details about an access point:
   a. Select the radio button that corresponds to the access point for which you want to see the details.
   b. Click **Details**.

      The AP Details pop-up screen displays. Because this is a tall screen that you need to scroll through, it is shown in the following two figures:





The following table describes the fields of the AP Details screen:

Item	Description
AP Info	
This information is self-explanatory.	
Profile Info For each security profile that is configured on the selected access point, the following information displays:	
Type	The type of profile (802.11b/bg/ng or 802.11a/na).
SSID	The wireless network SSID for the security profile.
Security	The security mode (Open, WEP, WPA, WPA2, or WPA/WPA2) for the security profile.
VLAN	The VLAN ID or VLAN name for the security profile.
Client Info The information that displays depends on the type and security of the connection that the client has to the access point. For each wireless client that is connected to the selected access point, some or all of the following information displays:	
MAC	The MAC address of the wireless client.
IP	The IP address of the client.
Channel	The channel that the wireless client is using to connect to the access point.

Item	Description
SSID	The wireless network SSID that the wireless client is using to connect to the access point.
Security	The security mode that the wireless client is using to connect to the access point (Open, WEP, WPA, WPA2, or WPA/WPA2).
Rogue AP Info For all rogue and unmanaged neighboring access points combined that are detected by the selected managed access point, the following information displays:	
Type	The type of profile that the rogue access point is using to connect to the access point (802.11b/bg/ng or 802.11a/na).
Reported	The total number of detected rogue access points in the wireless mode.
In Same Channel	The total number of detected rogue access points in the same channel.
In Interfering Channel	The total number of detected rogue access points in the interfering channel.
Statistics	
For each type of usage (Wired Ethernet, Wireless ng, bg, or b and Wireless na or a), statistics about transmitted and received packets and bytes display for the selected access point. The actual statistics are self-explanatory. **Note:** To see all fields of the table on the AP Details screen, scroll to the right.	

3. Click **OK**.

   The AP Details screen closes, and the Access Point screen displays again.

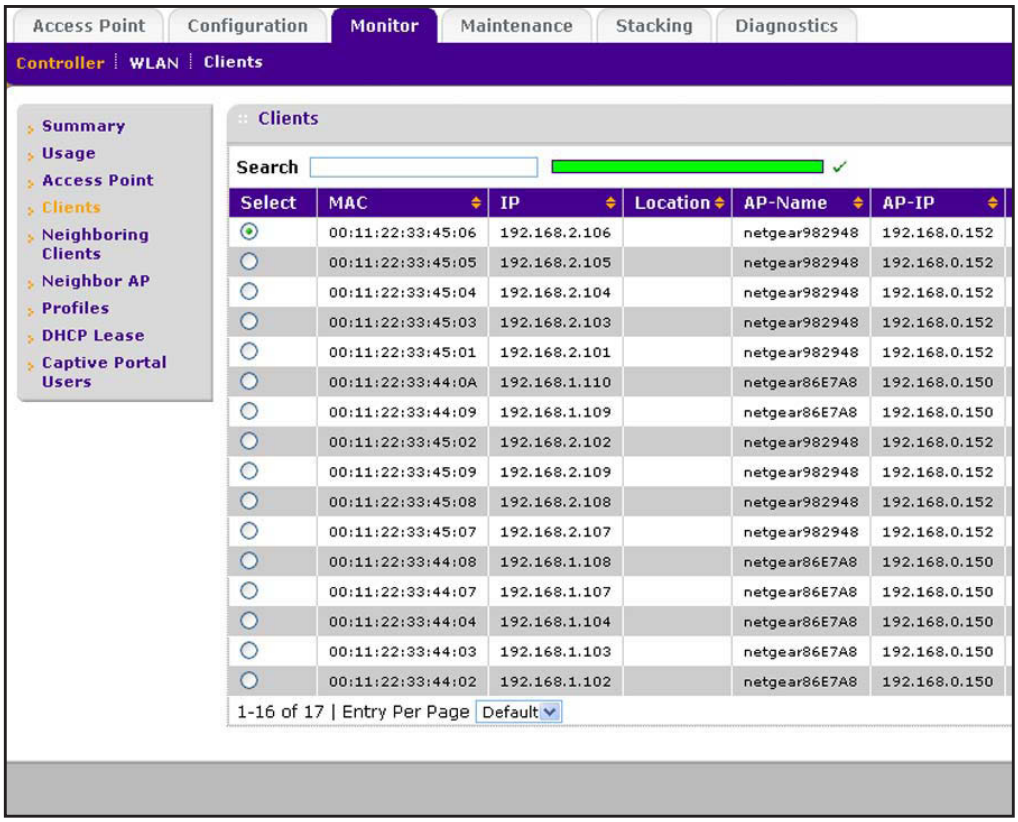
View Clients Managed by the Wireless Controller

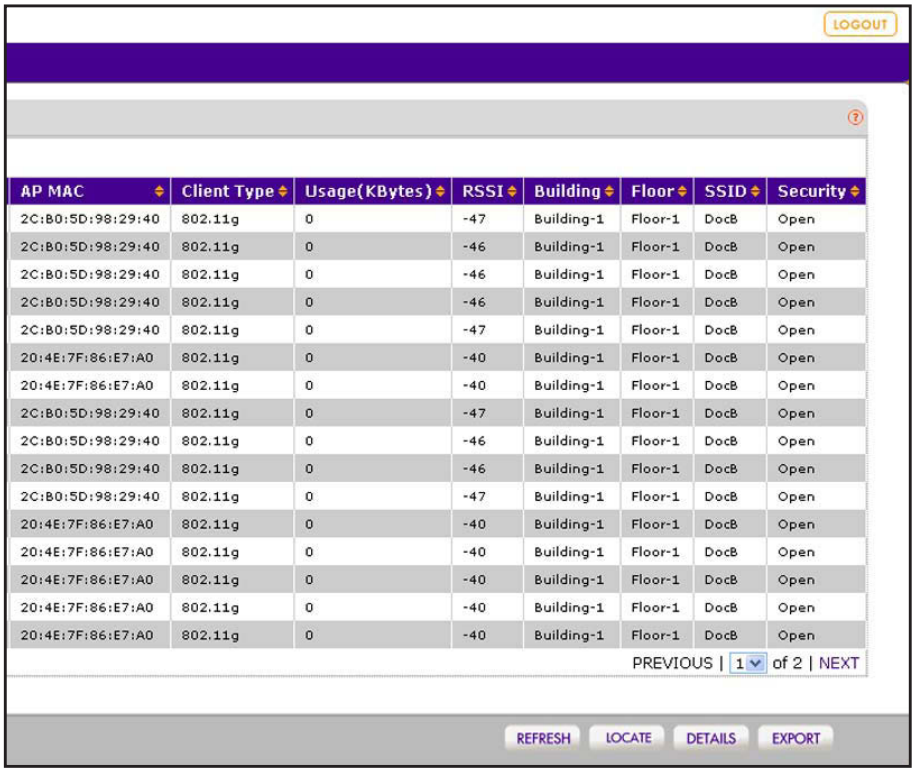
The Clients screen lets you view all clients that are connected to access points that are managed by the wireless controller.

➢ **To view the Clients screen:**

Select **Monitor > Controller > Clients**.

Because this screen is a wide screen, it is shown in the following two figures:



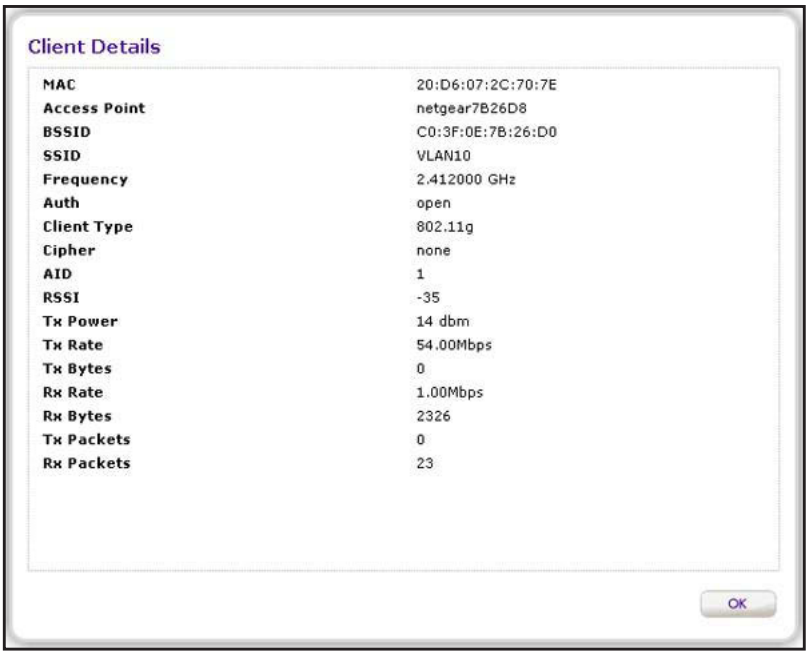


The following table describes the fields of the Clients table:

Item	Description
Select	The radio button that lets you select the client.
MAC	The MAC address of the wireless client.
IP	The IP address of the wireless client. Note the following: • If clients and the access point to which they are connected are in the same VLAN, all receive an IP address from the same DHCP server. • If clients and the access point to which they are connected are not in the same VLAN, you need to have a DHCP server for the client VLAN. • If clients are not connected to any DHCP server, IP addresses in the 169.254.x.x. range are assigned automatically.
Location	The location of the access point (see *Edit Access Point Information on the Managed AP List* on page 101) to which the wireless client is connected.
AP-Name	The name of the access point (see *Edit Access Point Information on the Managed AP List* on page 101) to which the wireless client is connected.
AP-IP	The IP address of the access point to which the wireless client is connected.
AP-MAC	The MAC address of the access point to which the wireless client is connected.
Client Type	The wireless mode that the wireless client is using to connect to the access point (802.11ng, 802.11 bg, 802.11 b, 802.11na, or 802.11 a).
Usage (KBytes)	The traffic usage of the wireless client in KB.
RSSI	The received signal strength indicator (RSSI) of the wireless client.
Building	The building designation is always Building-1.
Floor	The floor designation is always Floor-1.
SSID	The wireless network SSID that the wireless client is using to connect to the access point.
Security	The security mode (Open, WEP, WPA, WPA2, or WPA/WPA2) that the wireless client is using to connect to the access point.

4. (Optional) To see details about a client:
   a. Select the radio button that corresponds to the clients for which you want to see the details.
   b. Click **Details**.

The Client Details pop-up screen displays:



The following table describes the fields of the Client Details screen:

Item	Description
MAC	The MAC address of the wireless client.
Access Point	The name of the access point to which the wireless client is connected.
BSSID	The MAC address of the access point's radio to which the wireless client is connected.
SSID	The wireless network SSID that the wireless client is using to connect to the access point.
Frequency	The channel frequency that the wireless client is using to connect to the access point.
Auth	The security mode that the wireless client is using to connect to the access point (Open, WEP, WPA, WPA2, or WPA/WPA2).
Client Type	The wireless mode that the wireless client is using to connect to the access point (802.11ng, 802.11 bg, 802.11 b, 802.11na, or 802.11 a).
Cipher	The type of encryption that the wireless client is using (WEP, AES, TKIP, or TKIP + AES).
AID	The association ID of the client.
RSSI	The received signal strength indicator (RSSI) of the wireless client.
Tx Power	The transmit power of the wireless client.
Tx Rate	The transmit rate in Mbps of the wireless client.

Item	Description
Tx Bytes	The number of bytes that the wireless client transmitted.
Rx Rate	The receive rate in Mbps of the wireless client.
Rx Bytes	The number of bytes that the wireless client received.
Tx Packets	The number of packets that the wireless client transmitted.
Rx Packets	The number of packets that the wireless client received.

5. Click **Cancel**.

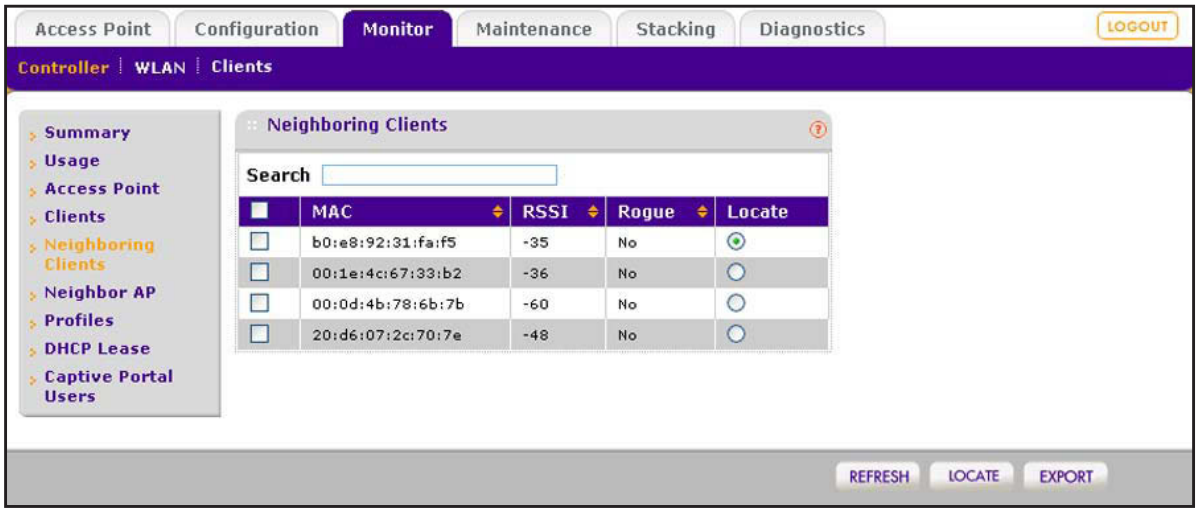
   The Client Details screen closes, and the Clients screen displays again.

View Neighboring Clients Detected by the Wireless Controller

The Neighboring Clients screen lets you monitor clients that the wireless controller detected and that are attached to known or rogue access points.

➢ **To view the Neighboring Clients screen:**

Select **Monitor > Controller > Neighboring Clients**.



The following table describes the fields of the Neighboring Clients table:

Item	Description
Locate	Not applicable. The location functionality will be added in a later release.
MAC	The MAC address of the neighboring client.

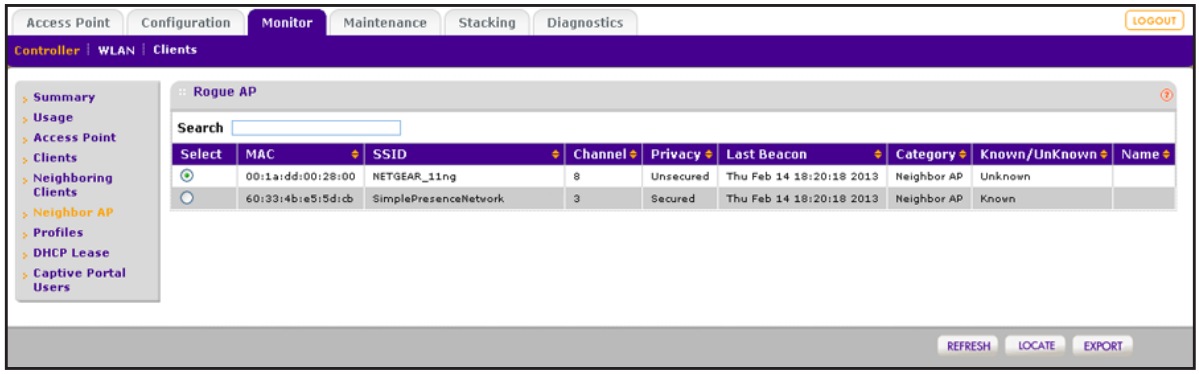
Item	Description
RSSI	The received signal strength indicator (RSSI) of the neighboring client.
Rogue	Shows whether or not (Yes or No) the neighboring client is connected to a rogue access point.

View Neighboring Access Points Detected by the Wireless Controller

The Rogue AP screen lets you monitor the access points that the wireless controller detected but that are not managed by the wireless controller.

➢ **To view the Rogue AP screen:**

Select **Monitor > Controller > Neighbor AP**.



The following table describes the fields of the Rogue AP table:

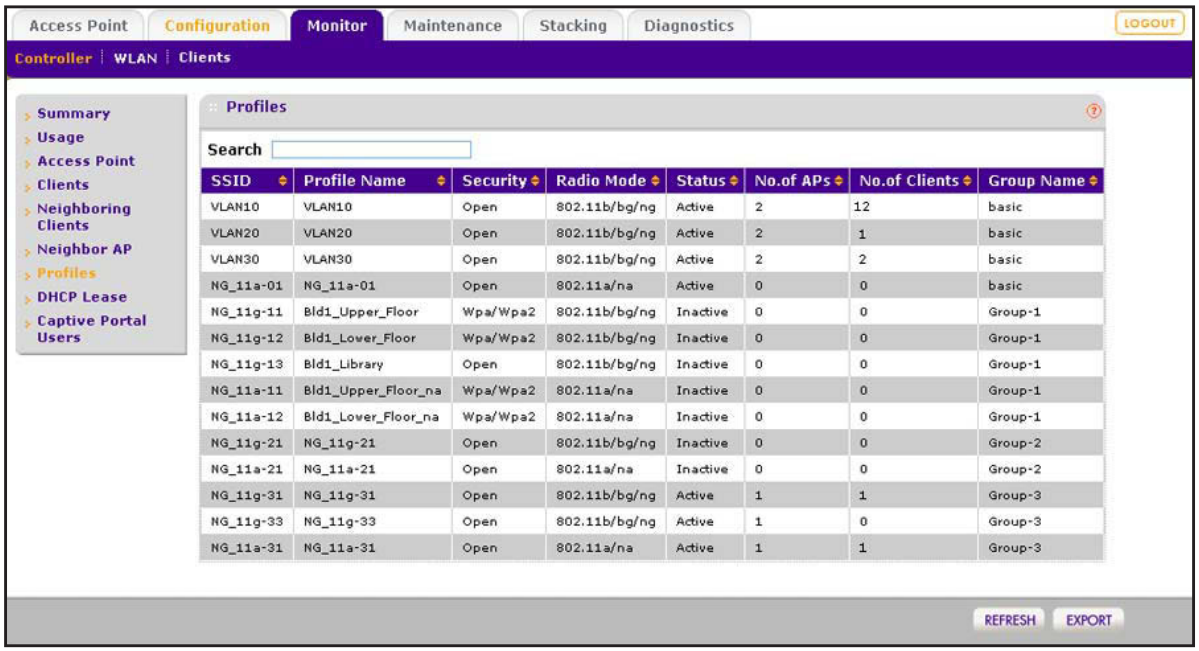
Item	Description
Select	The radio button that lets you select the access point.
MAC	The MAC address of the rogue access point.
SSID	The wireless network SSID that the rogue access point is using.
Channel	The channel that the access point is using.
Privacy	The security of the access point (Secured or Unsecured).
Last Beacon	The last beacon that the access point transmitted.
Category	The category that the access point belongs to (Neighbor AP or Rogue AP)
Known/Unknown	The status of the access point (Known or Unknown).
Name	The name of the access point, if a name is assigned.

View Security Profiles Managed by the Wireless Controller

The Profiles screen lets you monitor all security profiles on the access points that are managed by the wireless controller.

➢ **To view the Profiles screen:**

Select **Monitor > Controller > Profiles**.



The following table describes the fields of the Profiles table:

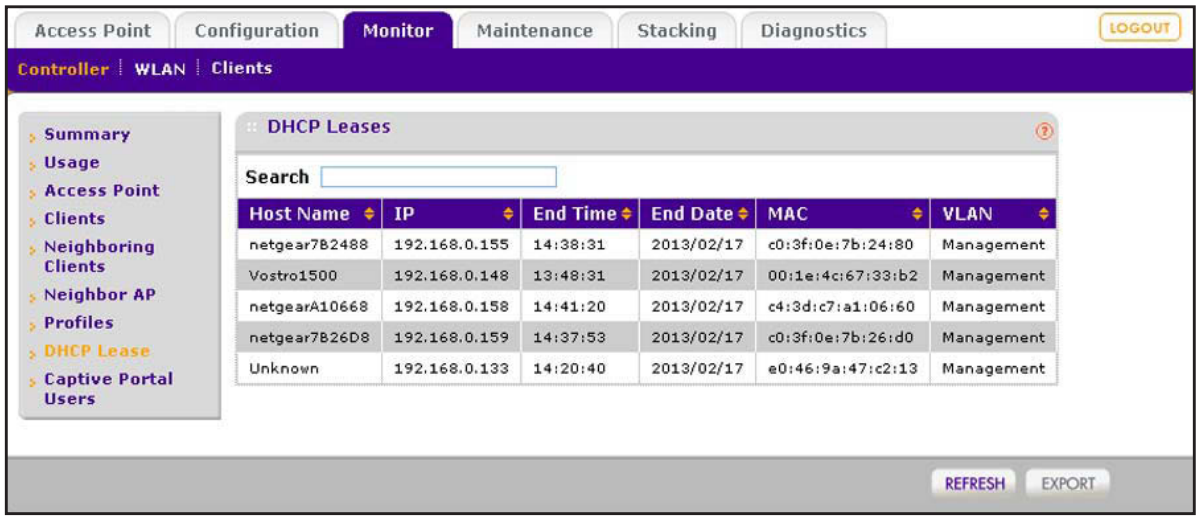
Item	Description
SSID	The wireless network SSID for the security profile.
Profile Name	The name of the security profile.
Security	The security mode (Open, WEP, WPA, WPA2, or WPA/WPA2) for the security profile.
Radio Mode	The wireless mode for the security profile (802.11b/bg/ng or 802.11a/na).
Status	The status of the security profile (Active or Inactive).
No.of APs	The number of access points that are attached to the security profile.
No.of Clients	The number of clients that are attached (through the access points) to the security profile.
Group Name	The name of the group of which the security profile is a member.

View DHCP Leases Provided by the Wireless Controller

The DHCP Leases screen displays the current DHCP clients that have been allocated IP addresses by the DHCP server on the wireless controller.

➢ **To view the DHCP Leases screen:**

Select **Monitor > Controller > DHCP Lease**.



The following table describes the fields of the DHCP Leases table:

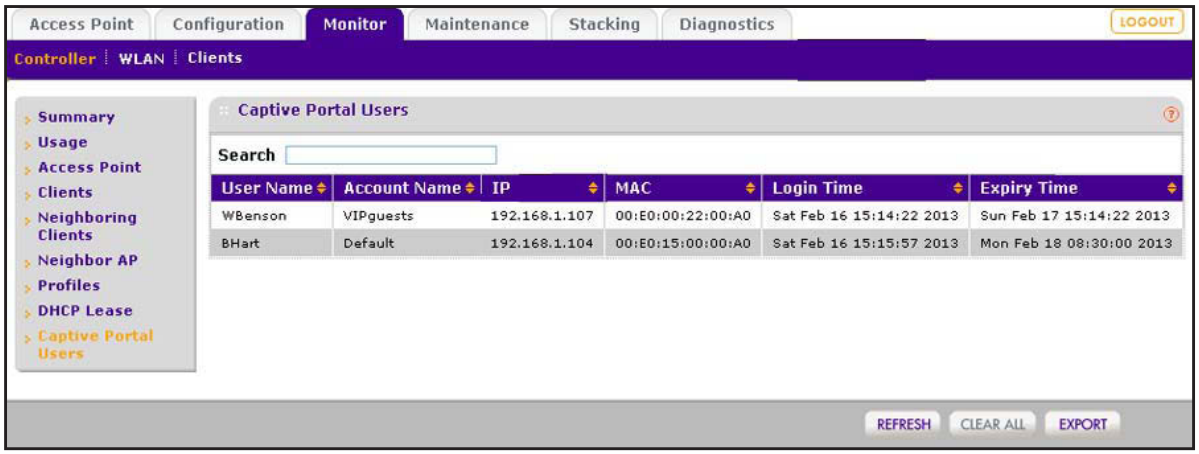
Item	Description
Host Name	The host name of the DHCP client.
IP	The IP address that is allocated to the DHCP client.
End Time	The DHCP lease end time for the DHCP client.
End Date	The DHCP lease end date for the DHCP client.
MAC	The MAC address of the DHCP client.
VLAN	The VLAN name or number that the DHCP server and DHCP client are using to connect.

View Captive Portal Users Managed by the Wireless Controller

The Captive Portal Users screen displays the current guests and users that are logged in to a captive portal on the access points that are managed by the wireless controller.

➢ **To view the Captive Portal Users screen:**

Select **Monitor > Controller > Captive Portal Users**.



The following table describes the fields of the Captive Portal Users table:

Item	Description
User Name	The login name of the user.
Account Name	The account name, if any, that is associated with the user.
IP	The IP address of the user.
MAC	The MAC address of the device with which the user is logged in.
Login Time	The time that the user logged in.
Expiry Time	The time when the login access expires.

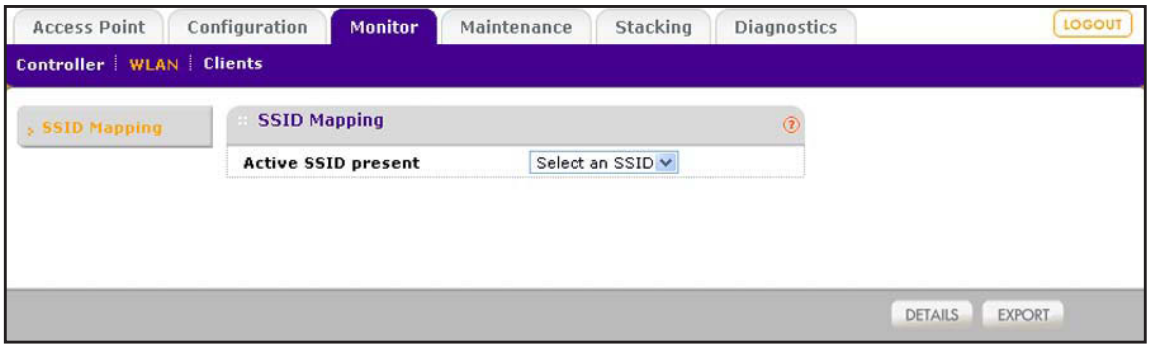
Monitor the SSIDs

The Active SSID table on the SSID Mapping screen lets you monitor all access points that function in an SSID.

➢ **To monitor an active SSID in the network:**

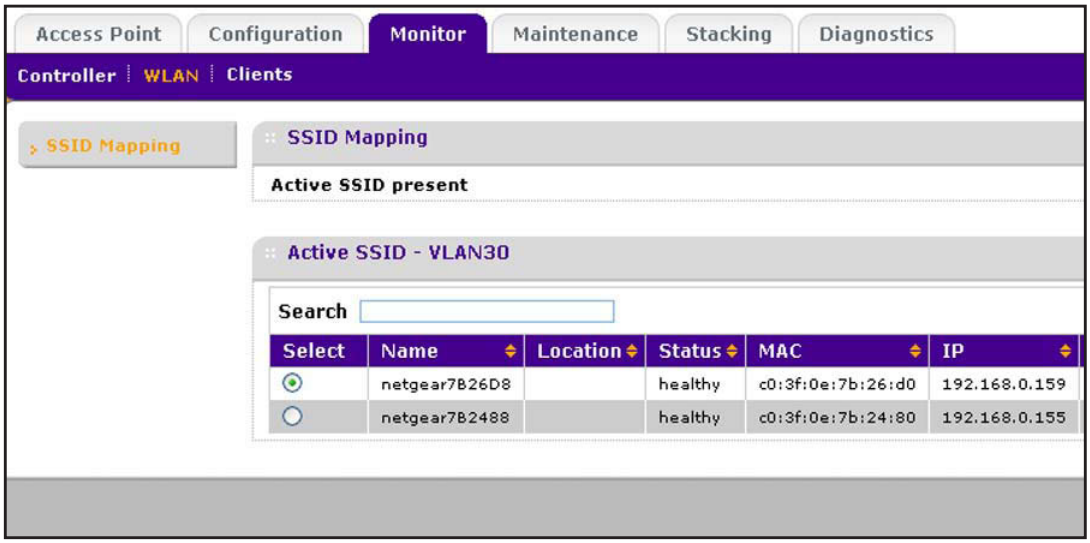
1. Select **Monitor > WLAN**.

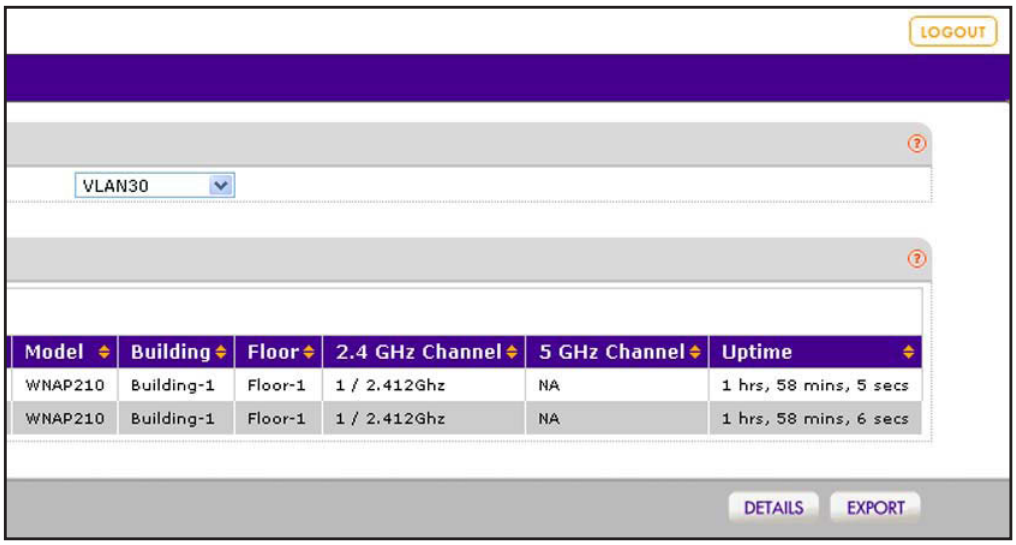
The SSID Mapping screen displays:



2. From the Active SSID present menu, select an SSID.

   The Active SSID table for the selected SSID displays. Because this screen is a wide screen, it is shown in the following two figures:



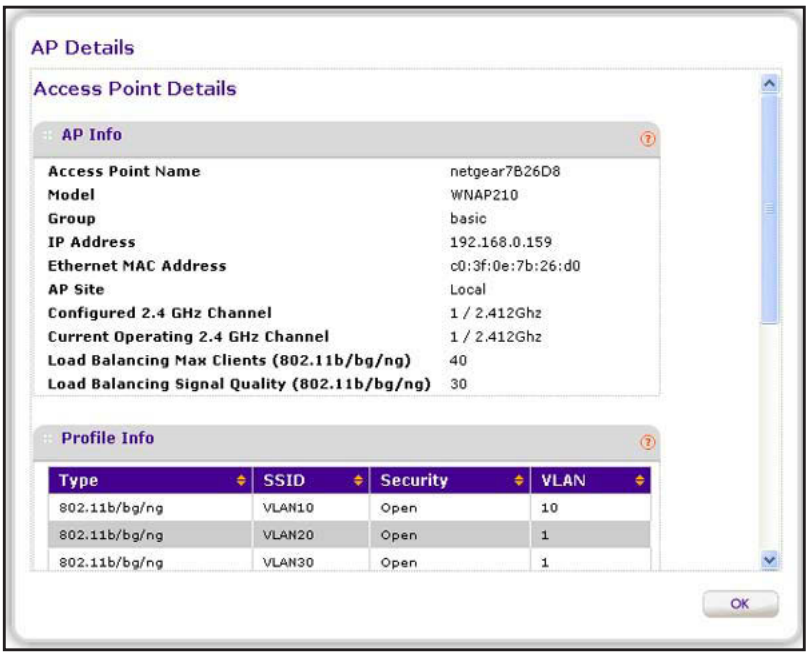


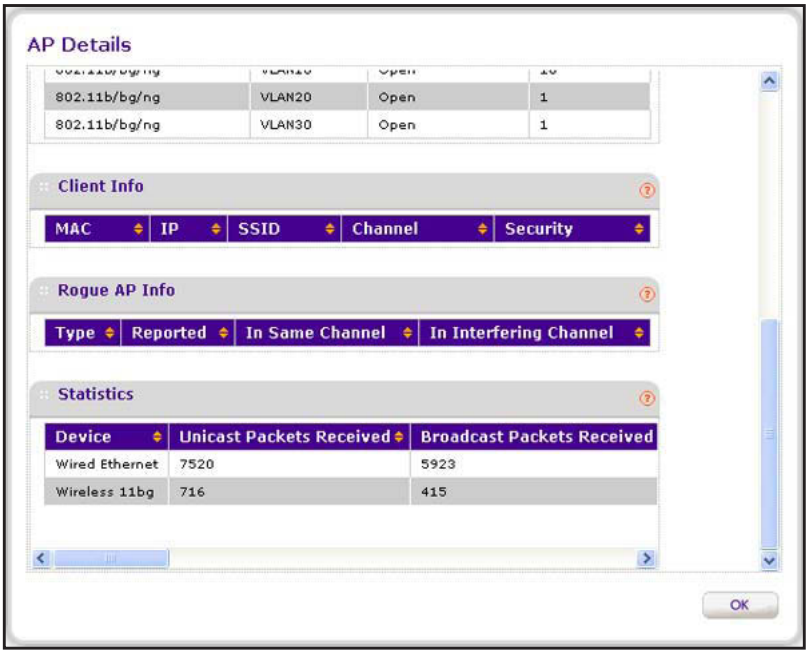
The following table describes the fields of the Active SSID table with access points:

Item	Description
Select	The radio button that lets you select the access point.
Location	The location of the access point (see *Edit Access Point Information on the Managed AP List* on page 101).
Name	The name of the access point (see *Edit Access Point Information on the Managed AP List* on page 101).
Status	The status of the access point (healthy or down).
MAC	The MAC address of the access point.
IP	The IP address of the access point.
Model	The model of the access point (WNAP210, WNAP320, WNDAP350, WNDAP360, or WNDAP380R).
Building	The building designation is always Building-1.
Floor	The floor designation is always Floor-1.
2.4 GHz Channel	The configured 2.4 GHz channel on the access point. This information can change after initial configuration of the access point because of automatic channel allocation.
5 GHz Channel	The configured 5 GHz channel on the access point. This information can change after initial configuration of the access point because of automatic channel allocation.
Uptime	The period since the access point was last restarted.

3. (Optional) To see details about an access point:
   a. Select the radio button that corresponds to the access point for which you want to see the details.
   b. Click **Details**.

The AP Details pop-up screen displays. Because this is a tall screen that you need to scroll through, it is shown in the following two figures:





The following table describes the fields of the AP Details screen:

Item	Description
AP Info	
This information is self-explanatory.	

Item	Description
Profile Info For each security profile that is configured on the selected access point, the following information displays:	
Type	The type of profile (802.11b/bg/ng or 802.11a/na).
SSID	The wireless network SSID for the security profile.
Security	The security mode (Open, WEP, WPA, WPA2, or WPA/WPA2) for the security profile.
VLAN	The VLAN ID or VLAN name for the security profile.
Client Info The information that displays depends on the type and security of the connection that the client has to the access point. For each wireless client that is connected to the selected access point, some or all of the following information displays:	
MAC	The MAC address of the wireless client.
IP	The IP address of the client.
Channel	The channel that the wireless client is using to connect to the access point.
SSID	The wireless network SSID that the wireless client is using to connect to the access point.
Security	The security mode that the wireless client is using to connect to the access point (Open, WEP, WPA, WPA2, or WPA/WPA2).
Rogue AP Info For all rogue and unmanaged neighboring access points combined that are detected by the selected managed access point, the following information displays:	
Type	The type of profile that the rogue access point is using to connect to the access point (802.11b/bg/ng or 802.11a/na).
Reported	The total number of detected rogue access points in the wireless mode.
In Same Channel	The total number of detected rogue access points in the same channel.
In Interfering Channel	The total number of detected rogue access points in the interfering channel.
Statistics	
For each type of usage (Wired Ethernet, Wireless ng, bg, or b and Wireless na or a), statistics about transmitted and received packets and bytes display for the selected access point. The actual statistics are self-explanatory. **Note:** To see all fields of the table on the AP Details screen, scroll to the right.	

4. Click **OK**.

   The AP Details screen closes, and the SSID Mapping screen displays again.

Monitor Local Clients

You can monitor the clients that have been accepted into the wireless network.

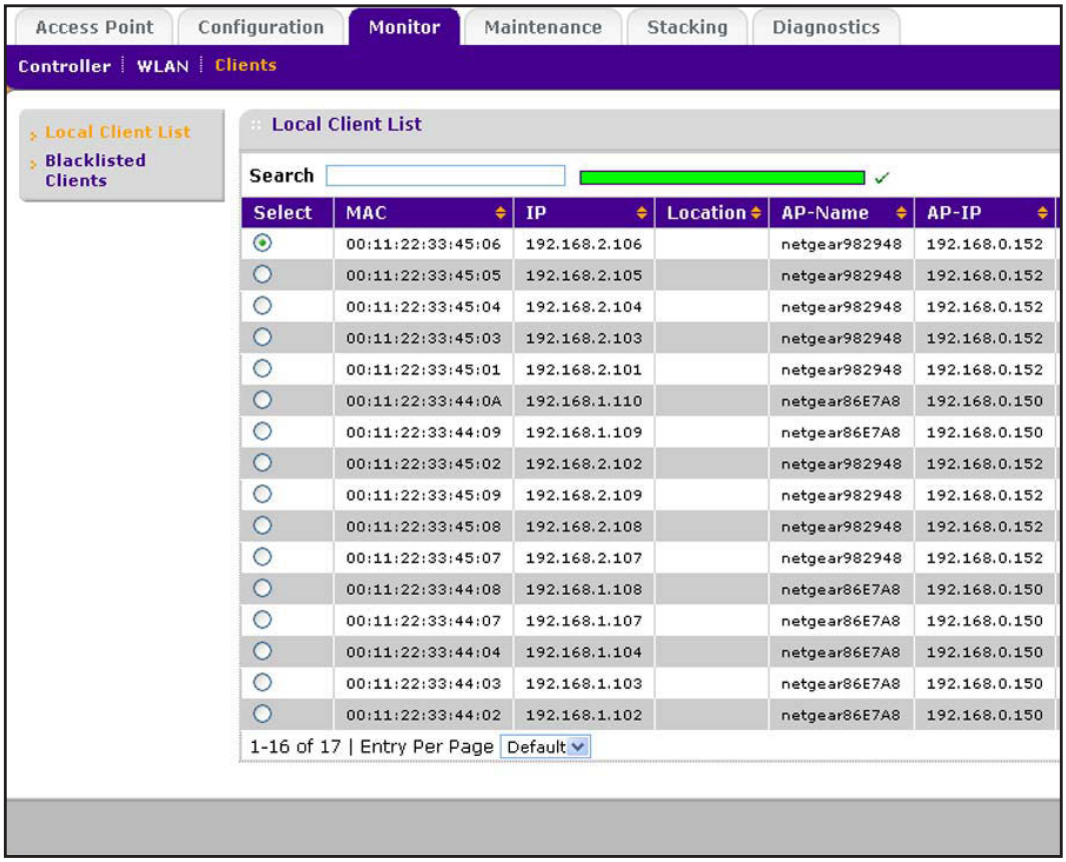
Note: Although the web management interface provides a Blacklisted Clients submenu link, monitoring of blacklisted clients is not supported. Monitoring of blacklisted clients will be supported in a future release.

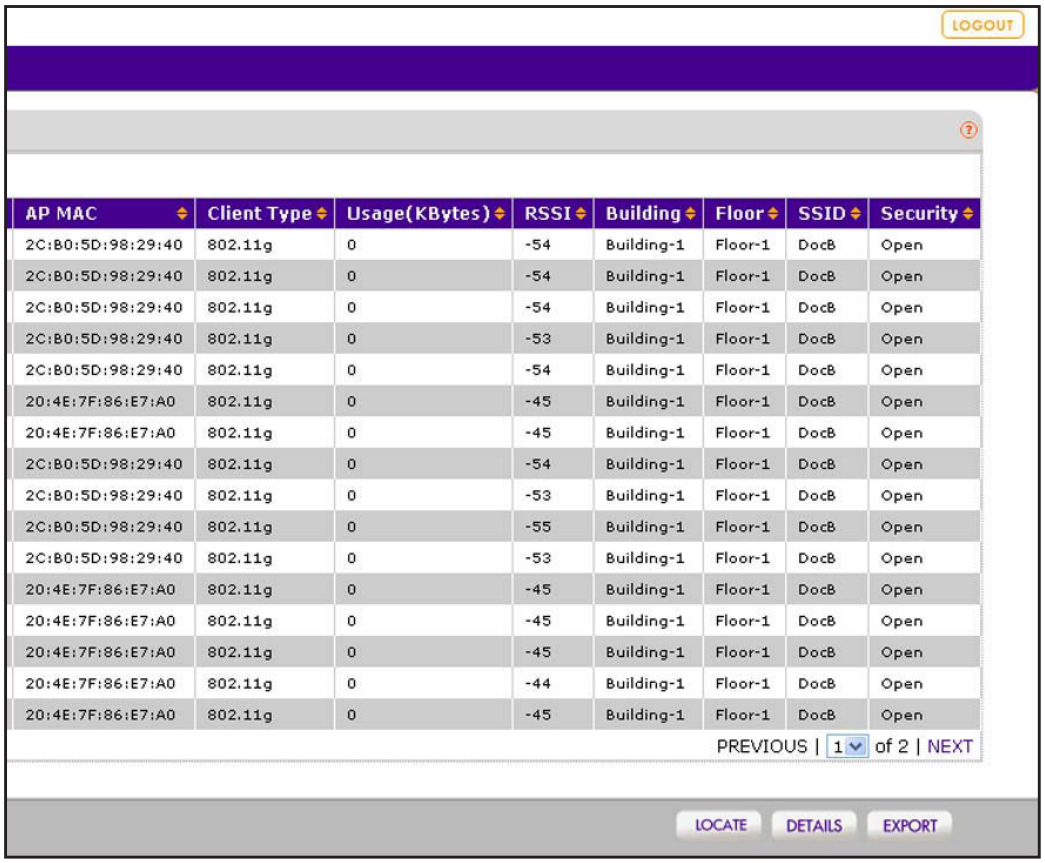
The Local Client List screen shows *all* clients in the network (that is, all clients managed by all wireless controllers in the network), whereas the Clients screen (see *View Clients Managed by the Wireless Controller* on page 180) shows only the clients that are managed by a single wireless controller.

Because this release does not support stacking, the information that is shown in the Local Clients screen is identical to the information that is shown in the Clients screen.

➢ **To view the clients in the network:**

1. Select **Monitor > Clients > Local Client List**. Because this screen is a wide screen, it is shown in the following two figures:





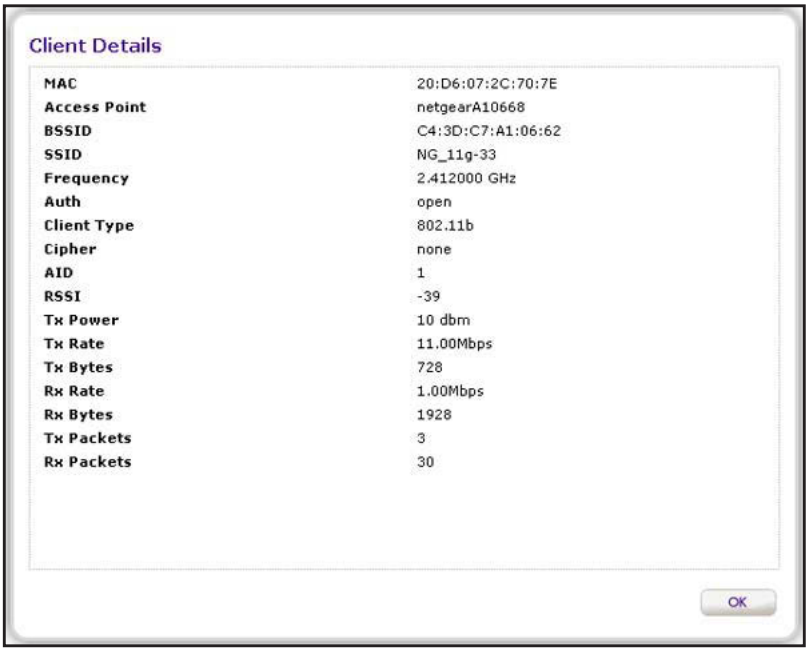
The following table describes the fields of the Clients table on the Local Client List screen:

Item	Description
Select	The radio button that lets you select the client.
MAC	The MAC address of the wireless client.
IP	The IP address of the wireless client.
Location	The location of the access point (see *Edit Access Point Information on the Managed AP List* on page 101) to which the wireless client is connected.
AP-Name	The name of the access point (see *Edit Access Point Information on the Managed AP List* on page 101) to which the wireless client is connected.
AP-IP	The IP address of the access point to which the wireless client is connected.
AP MAC	The MAC address of the access point to which the wireless client is connected.
Client Type	The wireless mode that the wireless client is using to connect to the access point (802.11ng, 802.11 bg, 802.11 b, 802.11na, or 802.11 a).
Usage (KBytes)	The traffic usage of the wireless client in KB.
RSSI	The received signal strength indicator (RSSI) of the wireless client.

Item	Description
Building	The building designation is always Building-1.
Floor	The floor designation is always Floor-1.
SSID	The wireless network SSID that the wireless client is using to connect to the access point.
Security	The security mode (Open, WEP, WPA, WPA2, or WPA/WPA2) that the wireless client is using to connect to the access point.

2. (Optional) To see details about a client:
   a. Select the radio button that corresponds to the clients for which you want to see the details.
   b. Click **Details**.

      The Client Details pop-up screen displays:



The following table describes the fields of the Client Details screen:

Item	Description
MAC	The MAC address of the wireless client.
Access Point	The name of the access point to which the wireless client is connected.
BSSID	The MAC address of the access point's radio to which the wireless client is connected.
SSID	The wireless network SSID that the wireless client is using to connect to the access point.

Item	Description
Frequency	The channel frequency that the wireless client is using to connect to the access point.
Auth	The security mode that the wireless client is using to connect to the access point (Open, WEP, WPA, WPA2, or WPA/WPA2).
Client Type	The wireless mode that the wireless client is using to connect to the access point (802.11ng, 802.11 bg, 802.11 b, 802.11na, or 802.11 a).
Cipher	The type of encryption that the wireless client is using (WEP, AES, TKIP, or TKIP + AES).
AID	The association ID of the client.
RSSI	The received signal strength indicator (RSSI) of the wireless client.
Tx Power	The transmit power of the wireless client.
Tx Rate	The transmit rate in Mbps of the wireless client.
Tx Bytes	The number of bytes that the wireless client transmitted.
Rx Rate	The receive rate in Mbps of the wireless client.
Rx Bytes	The number of bytes that the wireless client received.
Tx packets	The number of packets that the wireless client transmitted.
Rx Packets	The number of packets that the wireless client received.

3. Click **Cancel**.

   The Client Details screen closes, and the Local Client List screen displays again.

11 Troubleshooting

This chapter includes the following sections:

- *Troubleshoot Basic Functioning*
- *Troubleshoot the Web Management Interface*
- *Troubleshoot a TCP/IP Network Using the Ping Utility*
- *Use the Reset Button to Restore Default Settings*
- *Problems with Date and Time*
- *Problems with Access Points*
- *Use the Diagnostic Tools on the Wireless Controller*

Troubleshoot Basic Functioning

After you turn on power to the wireless controller, the following sequence of events should occur:

1. When power is first applied, verify that the Power LED is lit green and that the Status LED is lit yellow.
2. After approximately two minutes, verify the following:
   a. The Status LED is lit green.
   b. The left Ethernet port LED is lit for any local port that is connected.

   If the port's left LED is lit, a link has been established to the connected device. If the port is connected to a 1000 Mbps device, verify that the port's right LED is green. If the port functions at 100 Mbps, the right LED is yellow. If the port functions at 10 Mbps, the right LED is off.

If any of these conditions do not occur, see to the appropriate following section.

Power LED Is Not Lit

If the Power and other LEDs are off when your wireless controller is turned on, make sure that the power cord is correctly connected to your wireless controller and that the power supply adapter is correctly connected to a functioning power outlet.

If the error persists, you have a hardware problem and should contact NETGEAR technical support.

Status LED Never Turns Off

When the wireless controller is powered on, the Status LED is lit yellow for approximately two minutes and then turns green when the wireless controller has completed its initialization. If the Status LED remains yellow, a fault has occurred within the wireless controller.

If the Status LED is yellow more than several minutes minute after power-up:

- Turn off the power, and turn it on again to see if the wireless controller recovers.
- Reset the wireless controller's configuration to factory default settings. Doing so sets the wireless controller's IP address to **192.168.0.250**. For more information, see *Reboot or Reset the Wireless Controller* on page 156.

If the error persists, you might have a hardware problem and should contact NETGEAR technical support.

Ethernet Port LEDs Are Not Lit

If the Ethernet LEDs do not light when the Ethernet connection is made, check the following:

- Make sure that the Ethernet cable connections are secure at the wireless controller and at the hub, switch, or router.
- Make sure that power is turned on to the connected hub, switch, or router.
- Be sure that you are using the correct cables.

Troubleshoot the Web Management Interface

If you are unable to access the wireless controller's web management interface from a computer on your local network, try to isolate the problem. You can most likely solve the problem by following the suggestions that are described in the following sections.

Ethernet Cabling

Check the Ethernet connection between the computer and the wireless controller as described in the previous section (see *Ethernet Port LEDs Are Not Lit*).

IP Address Configuration

- Make sure that your computer's IP address is on the same subnet as the wireless controller. If you are using the recommended addressing scheme, make sure that your computer has a static IP address of 192.168.0.210 and a subnet of 255.255.255.0.

> **Note:** If your computer's IP address is shown as 169.254.x.x: Windows and Mac operating systems generate and assign an IP address if the computer cannot reach a DHCP server. These autogenerated addresses are in the range of 169.254.x.x. If your IP address is in this range, check the connection from the computer to the wireless controller and reboot your computer.

- If the wireless controller's IP address has been changed and you do not know the current IP address, reset the wireless controller's configuration to factory default settings. This sets the wireless controller's IP address to 192.168.0.250. For more information, see *Reboot or Reset the Wireless Controller* on page 156.

If you do not want to revert to the factory default settings and lose your configuration settings, you could use one of the following methods to discover the IP address of the wireless controller:

- Reboot the wireless controller and use a sniffer to capture packets sent during the reboot. Look at the ARP packets to locate the wireless controller's LAN interface address.
- Run an IP scanner application in your network to discover the IP address of the wireless controller.
- Connect a serial cable between a computer and the wireless controller, and use the `ipconfig` command to discover the IP address of the wireless controller.

Internet Browser

- Make sure that you are using the http://address login rather than the https://address login.
- Make sure that your browser has Java, JavaScript, or ActiveX enabled. If you are using Internet Explorer, click **Refresh** to be sure that the Java applet is loaded.
- Try quitting the browser and launching it again.
- Make sure that you are using the correct login information. The factory default login name is admin, and the password is password. Make sure that Caps Lock is off when entering this information.

If the wireless controller does not save changes you have made in the web management interface, check the following:

- When entering configuration settings, be sure to click the **Apply** button before moving to another tab or screen, or your changes are lost.
- Click the **Refresh** or **Reload** button in your web browser. The changes might have occurred, but the web browser might be caching the old configuration.

After you have upgraded the firmware, if the browser does not display the latest features of the web management interface, clear the browser's cache, and refresh the screen.

Troubleshoot a TCP/IP Network Using the Ping Utility

Most TCP/IP terminal devices and routers contain a ping utility that sends an echo request packet to the designated device. The device then responds with an echo reply. You can easily troubleshoot a TCP/IP network by using the ping utility in your computer.

You can ping the wireless controller from your computer to verify that the LAN path to your wireless controller is set up correctly.

➢ **To ping the wireless controller from a computer running Windows:**

1. From the Windows toolbar, click the **Start** button, and select **Run**.

2. In the field provided, type **ping** followed by the IP address of the wireless controller, as in this example:

   ping 192.168.0.250

3. Click **OK**.

   You should see a message like this one:

   ```
   Pinging <IP address> with 32 bytes of data
   ```

   If the path is working, you see this message:

   ```
   Reply from < IP address >: bytes=32 time=NN ms TTL=xxx
   ```

   If the path is not working, you see this message:

   ```
   Request timed out
   ```

   If the path is not functioning correctly, you could have one of the following problems:

- Wrong physical connections

  Make sure that the Ethernet LEDs are lit. If they are off, follow the instructions in *Ethernet Port LEDs Are Not Lit* on page 199.

- Wrong network configuration
  - Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your computer.
  - Verify that the IP address for your wireless controller and your computer are correct and that the addresses are on the same subnet.

Use the Reset Button to Restore Default Settings

If you can access the wireless controller, you can use the Reboot/Reset Controllers screen (the path is Maintenance > Backup/Restore) to perform a soft or hard reset (see *Reboot or Reset the Wireless Controller* on page 156).

If you can no longer access the wireless controller, press the **Reset** button on the front panel (see *Front Panel Ports, Slots, and LEDs* on page 11) to restore the factory default settings.

➢ **To clear all data and restore the factory default values:**

1. Press and hold the **Reset** button for about eight seconds until the Status LED turns on and begins to blink.
2. Release the **Reset** button. The reboot process is complete after several minutes when the Status LED on the front panel goes off.

Note: After restoring the factory default configuration, the wireless controller's default LAN IP address is 192.168.0.250, the default login user name is admin, and the default login password is password.

Problems with Date and Time

The Time Settings screen displays the current date and time of day (see *Manage the Time Settings* on page 48). The wireless controller uses the Network Time Protocol (NTP) to obtain the current time from one of several network time servers on the Internet. Each entry in the log is stamped with the date and time of day.

When the date shown is January 1, 2000, the wireless controller has not yet successfully reached a network time server. Verify that the wireless controller can reach the Internet. If you have just completed configuring the wireless controller, wait at least five minutes and check the date and time again.

Problems with Access Points

If you encounter access point discovery or connection problems, the information in this section might help you to resolve these problems.

Discovery Problems

If the wireless controller does not discover any or all access points, check the following:

For all access points:

- Make sure that the wireless controller is connected to the LAN (see *Ethernet Port LEDs Are Not Lit* on page 199).
- Make sure that you have entered the correct IP range if the access points function in different VLANs, are behind an IP subnet, or are already installed and working in standalone mode (see *Access Point Discovery Guidelines* on page 91).
- Make sure that the access points run at least their initial firmware release or a newer version. For firmware requirements, see *NETGEAR ProSAFE Access Points* on page 15.

For local access points that are installed across a Layer 3 network:

- Verify that access points that are already installed and working in standalone mode have SSH and SNMP enabled (which is the default setting).
- Make sure that UDP port number 7890 is unblocked in the firewall.
- Except for access points in factory default state that are in the same Layer 2 network, if more than one access point has the same IP address, only one of them is discovered at a time. You have to add the access point to the managed list, change its IP address, and run discovery again to discover the next access point with that IP address.
- Make sure that DHCP option 43 (vendor-specific information) is enabled on an external DHCP server. (Specifying an internal DHCP server on the wireless controller automatically enables DHCP option 43 with the IP address of the wireless controller.)

For more information, see *Access Point Discovery Guidelines* on page 91.

Connection Problems

When an access point is converted from standalone AP mode to managed AP mode, its static IP address is changed to an IP address that is issued by the DHCP server, either one in the network or one that is configured on the wireless controller. This occurs to ensure that each managed access point has a unique IP address.

If there is no DHCP server or if the access point cannot reach the DHCP server, the access point remains in the Connecting state, attempting to obtain an IP address. If there is no DHCP server in the network, configure one on the wireless controller (see *Manage the DHCP Server* on page 51). When a DHCP server becomes available, the access point can transition from the Connecting state to the Connected state.

Network Performance and Rogue Access Point Detection

When rogue access point detection is enabled, access points intermittently go off channel for short periods, which can affect network performance. The default rogue access point detection interval is 30 minutes. This interval is not configurable.

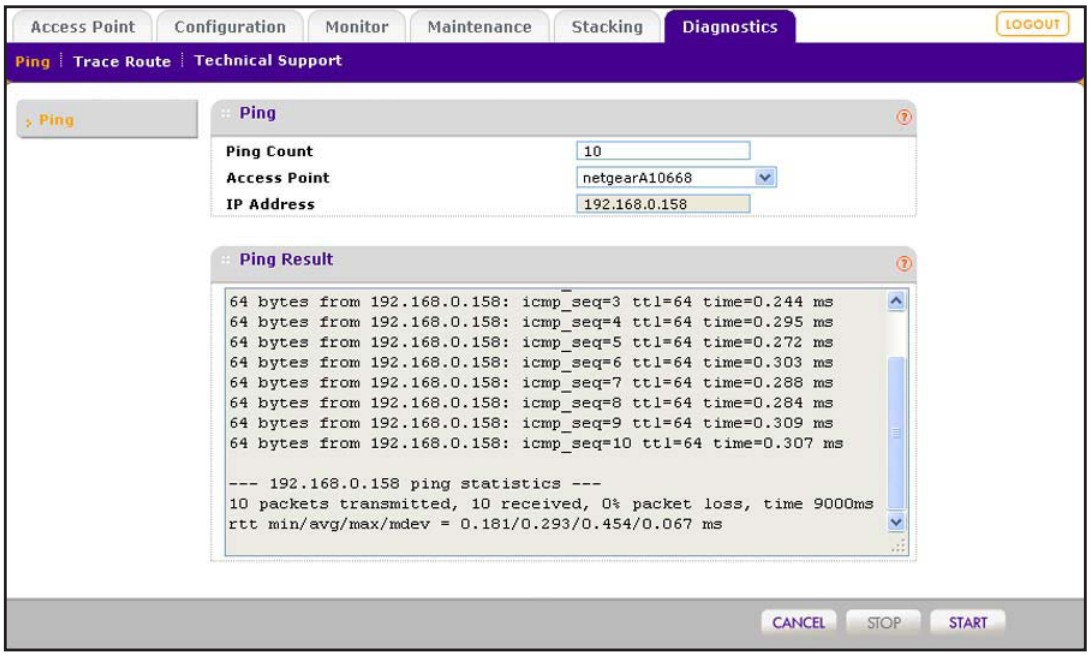
Use the Diagnostic Tools on the Wireless Controller

As part of the diagnostics functions on the wireless controller, you can ping a managed access point from the wireless controller or trace its route from the wireless controller.

➢ **To ping an access point:**

1. Select **Diagnostics > Ping**.

   The Ping screen displays:



2. In the Ping Count field, enter the number of ping packets to be sent.

   The default number is 10.

3. From the Access Point menu, select the access point to be pinged.

   After you have made your selection, the IP address of the access point displays in the IP Address field.

4. Click **Start**.

   The results are shown in the Ping Result field.

➢ **To trace a route to an access point:**

1. Select **Diagnostics > Trace Route**.

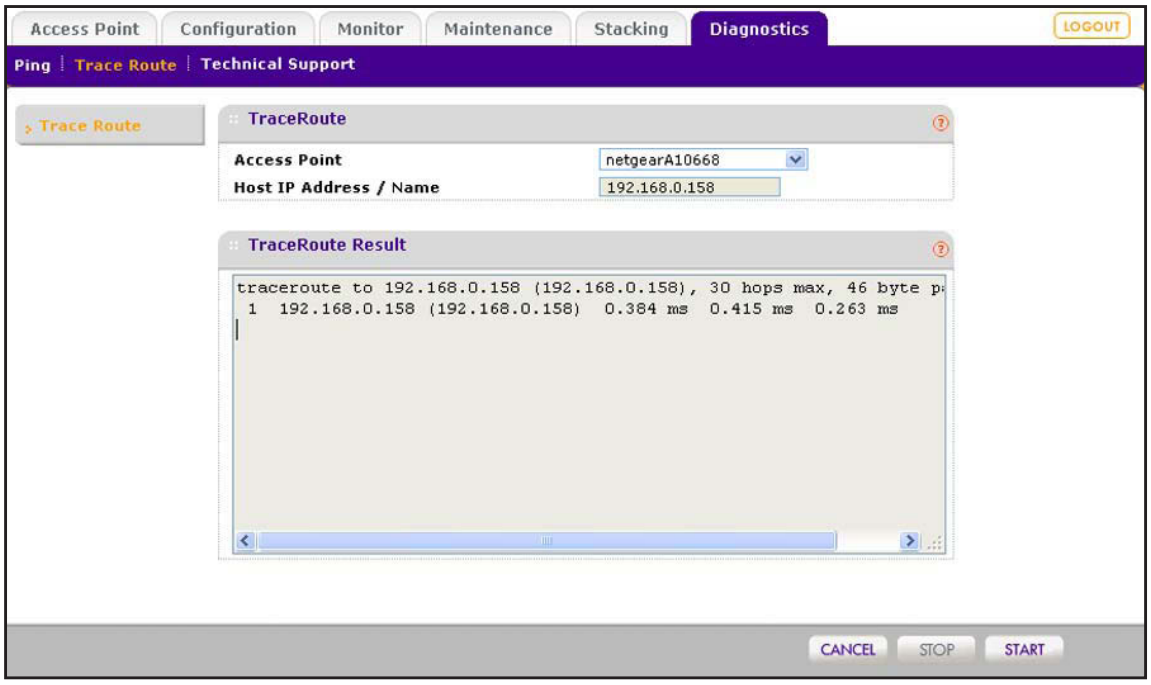
   The Trace Route screen displays (see the following figure).

2. From the Access Point menu, select the access point for which you want to trace the route.

   After you have made your selection, the IP address of the access point displays in the IP Address field.

3. Click **Start**.

   The results are shown in the TraceRoute Result field.



Factory Default Settings and Technical Specifications

A

This appendix includes the following sections:

- *Factory Default Settings*
- *Technical Specifications*
- *Password Requirements*

Factory Default Settings

You can restore the wireless controller to its factory default settings on the Reboot/Reset Controllers screen (see *Reboot or Reset the Wireless Controller* on page 156) or by using the Reset button on the front panel (see *Use the Reset Button to Restore Default Settings* on page 201). The wireless controller returns to the factory configuration settings that are shown in the following table:

Table 4. Factory default settings for the wireless controller

Feature		Default Setting
Login	User login URL	http:192.168.0.250
	User name (case-sensitive)	admin
	Login password (case-sensitive)	password
LAN	LAN IP	192.168.0.250
	Subnet mask	255.255.255.0
	Default gateway	192.168.0.1
	DHCP server pools	None
	Time zone	USA Pacific Standard Time (PST)
	Time zone adjusted for daylight saving time	Enabled
	SNMP	Enabled

Technical Specifications

The following table lists the technical and physical specifications.

Table 5. Technical and physical specifications

Feature	Default Setting
Electrical specifications	• 100–240V, 5A, 47–63 Hz, universal input with IEC 320 connector • Typical power consumption 165 W
Dimensions (W x H x D) cm	43 cm x 4.3 cm x 44 cm (Fits in a 1U rack)
Dimensions (W x H x D) in.	16.92 in. x 1.7 in. x 17.32 in. (Fits in a 1U rack)
Weight	• With one power supply: 6.32 kg (13.94 lb) • With an optional second power supply: 7.57 kg (16.68 lb)
Operating temperatures	0° to 45°C (32° to 113°F)
Operating humidity	90% maximum relative humidity

Table 5. Technical and physical specifications (continued)

Feature	Default Setting
Storage temperatures	–20° to 70°C (–4° to 158°F)
Storage humidity	95% maximum relative humidity, noncondensing
Major regulatory compliance	CCC

Note: For more information, see the *ProSAFE Wireless Controller WC9500* data sheet at *http://support.netgear.com/product/WC9500*.

Password Requirements

The following table lists the password requirements.

Table 6. Password requirements

Web Management Interface Path	User Type or Data Encryption	Restrictions		Section in This Manual
		Allowed Characters	Length	
Select **Maintenance > User Management**.	• Administrator • Read Only • Guest Provisioning • License Management Only	Alphanumerics and special characters	Up to 31	See *Manage Users, Accounts, and Passwords* on page 116.
1. Select **Maintenance > User Management**. 2. Click the **Captive Portal Users** tab.	Captive portal user	Alphanumerics and special characters	Up to 31	
1. Select **Maintenance > User Management**. 2. Click the **WiFi Clients** tab.	WiFi user	Alphanumerics only	Up to 31	

Table 6. Password requirements (continued)

Web Management Interface Path		User Type or Data Encryption	Restrictions		Section in This Manual
			Allowed Characters	Length	
Basic profile: 1. Select **Configuration > Profile > Basic > Radio**. 2. Select a profile. 3. Make a selection from the Network Authentication menu.	Shared Key	64-bit WEP	Hexadecimal	10 fixed	See *Configure Security Profiles for the Basic Profile Group* on page 67.
		128-bit WEP	Hexadecimal	26 fixed	
		152-bit WEP	Hexadecimal	32 fixed	
	WPA-PSK	TKIP	Alphanumerics and special characters, excluding quotes	Up to 63	
		TKIP + AES			
	WPA2-PSK	AES			
		TKIP + AES			
	WPA-PSK & WPA2-PSK	TKIP + AES			
Advanced profile: 1. Select **Configuration > Profile > Advanced > Radio**. 2. Select a group. 3. Click **Edit**. 4. Select a profile. 5. Make a selection from the Network Authentication menu.	Shared Key	64-bit WEP	Hexadecimal	10 fixed	See *Configure Security Profiles for Advanced Profile Groups* on page 71.
		128-bit WEP	Hexadecimal	26 fixed	
		152-bit WEP	Hexadecimal	32 fixed	
	WPA-PSK	TKIP	Alphanumerics and special characters, excluding quotes	Up to 63	
		TKIP + AES			
	WPA2-PSK	AES			
		TKIP + AES			
	WPA-PSK & WPA2-PSK	TKIP + AES			
Select **Configuration > Security > Authentication Server**.	External RADIUS Server	Shared Secret	Alphanumerics and special characters	Up to 127	See *Manage Authentication Servers and Authentication Server Groups* on page 85.
	External LDAP Server	Domain Admin User	Alphanumerics and special characters	Up to 32	

Index

Numerics

1U rack 206
2.4 GHz and 5 GHz channels 139
802.11 wireless modes 130, 134
802.1Q VLAN header 23, 49

A

AC power supplies 14
access point profile groups
  adding advanced groups 71
  assigning access points to 104
  basic and advanced, described 21
  channels and transmission power, overriding 131, 135
  profiles, adding and configuring 67, 73
  QoS, configuring 144
  radio, turning on and off 126
  rate limiting, configuring 148
  RF management, configuring 140
  wireless settings, configuring 128
access points
  adding 94, 98
  antennas, configuring 103
  autodiscovery 90
  channel allocation
    automatic 137–139
    manual 132, 137
  DHCP client, disabling 103
  discovery 91
  dual-band 15, 21, 64, 149
  factory default state, autodiscovery 92
  firmware, minimum version 15
  floor and building settings 103
  IP addresses 103
  IP subnet 92, 94
  known and unknown 110
  local 91, 98, 101
  managed status 101
  models, supported 15
  pinging 203
  rebooting 167
  remote 94, 98, 101
  rogue
    detecting and managing 108
    viewing on the managed access point 180, 192
    viewing on the wireless controller 185
  standalone mode
    autodiscovery 96
    returning to 104
  supported models 15
  tracing a route 204
  troubleshooting 202
  Tx power
    automatically controlling 141, 143
    manually controlling 133, 137
    overriding 131, 135
  viewing
    on the wireless controller 177
    security profiles 179, 192
    statistics 180, 192
  VLAN settings 103
access, remote 157
accounts, captive portal 116
active SSIDs, viewing 190
active voice calls, preventing channel allocation 139
Advanced Encryption Standard (AES) 79
advanced profile groups
  adding groups 71
  assigning access points to 104
  channels and transmission power, overriding 135
  described 21
  profiles, adding and configuring 73
  QoS, configuring 144
  radio, turning on and off 127
  rate limiting, configuring 150
  RF management, configuring 142
  wireless settings, configuring 133
advanced settings, description 20, 64
AES (Advanced Encryption Standard) 79
aggregated MAC protocol data unit (AMPDU) 131, 135
aggregation length 130, 135
AIFS (arbitration inter-frame space) 146
alarms
  settings 61
  viewing on the wireless controller 174
alerts, viewing and saving 163
AMPDU (aggregated MAC protocol data unit) 131, 135

antenna 103
arbitration inter-frame space (AIFS) 146
architecture, advanced profile group 22
authentication
  certificates 57
  external
    MAC authentication 69, 75, 81
    RADIUS and LDAP servers 79, 85–87, 114
  internal 88
  methods supported 24
  servers 85
autodiscovery, access points 90
automatic channel allocation and transmission power, WLAN healing 140

B

background QoS queue 144
backing up the configuration 152
basic profile group
  assigning access points to 104
  channels and transmission power, overriding 131
  described 21
  profiles, adding and configuring 67
  radio, scheduling 126
  rate limiting, configuring 149
  RF management, configuring 141
  wireless settings, configuring 128
basic service set identifier (BSSID) 108
basic settings, description 20, 64
beacon interval 130, 135
best effort QoS queue 144
bottom label 14
broadcasting SSID 69, 74
browsers
  supported 39
  troubleshooting 200
BSSID (basic service set identifier) 108

C

cabling, troubleshooting 199
calls, preventing channel allocation 139
captive portal
  accounts and users, adding 119–122
  configuring 111–115
  enabling 76
captive portal accounts and users, viewing 188
certificates, authentication 57
channel allocation
  automatic 137–139
  manual 132, 137
channel width 130, 134
classify rogue access points 109
client separation 69, 75
client VLANs 24, 27
clients, DHCP 103
clients, viewing
  in the network 194
  neighboring in the network 184
  on the access point 179, 192
  on the wireless controller 174, 182
clients, wireless, maximum number 147
color coding, channels 178
community names, SNMP 158
compliance, regulatory 207
configuration roadmaps 42–44
configuration, backing up and restoring 152–153
connection problems, troubleshooting 203
connectivity test 23
console port 12
contents, package 11
corporate channels 139
counter 12
country and region of operation 47
coverage hole detection 142, 144
customer information, licenses 56
CwMin and CwMax (minimum or maximum contention window) 146

D

data encryption
  configuring 69, 75
  supported methods 24
data rate 130, 134
data sheet 207
date, troubleshooting 202
default profile group. *See* basic profile group.
default settings 12, 201, 206
delivery traffic indication message (DTIM) interval 131, 135
detecting rogue access points 108
DHCP client, access points 103
DHCP leases, viewing 187
DHCP option 43 91
DHCP server
  description 24
  settings 52
diagnostic tools 203
digital counter 12
dimensions, wireless controller 206

discovering access points 91
discovery problems, troubleshooting 202
DNS servers 50
DTIM (delivery traffic indication message) interval 131, 135
dual-band access points 15, 21, 64, 149

E

EAP (Extensible Authentication Protocol) 119
electrical specifications 206
email notification server 62
encryption, methods supported 24
end user license agreement (EULA) 114
Ethernet port 12
Ethernet port LEDs
  described 13
  troubleshooting 199
EULA (end user license agreement) 114
event tracing 59
Extensible Authentication Protocol (EAP) 119
external antenna 103
external authentication
  MAC authentication 69, 75, 81
  RADIUS and LDAP servers 79, 85–87, 114

F

factory default settings, wireless controller 12, 201, 206
factory default state, access point autodiscovery 92
Fan LED, described 13
fans 14
features, overview 9, 16
firmware
  minimum version for access points 15
  multicast, using for access point upgrade 168
  upgrading, wireless controller 153
fragmentation length 130, 135
FTP server, firmware upgrade 154

G

GBICs (gigabit interface converters) 12
guard interval 130, 134
guest portal, configuring 111–115
GUI
  layout 41
  troubleshooting 199

H

hard reset 156, 201
healing, WLAN 140
high traffic load, preventing channel allocation 139
hotspot users 111
humidity, operating and storage 206

I

interference sources 23
internal antenna 103
internal authentication server 88
internal RADIUS server 85
inventory, licenses 165
IP addresses
  access points 103
  DHCP server assignment 52
  license server 55
  multicast range 169
  SNMP manager 158
  syslog server 60
  TFTP and FTP servers 155
  wireless controller 50
IP settings
  access points 103
  wireless controller 50
IP subnets
  access points 92, 94
  LAN 50
  troubleshooting 202

K

keys, licenses 57, 166
known rogue access points 110

L

label, bottom 14
LAN path, troubleshooting 200
LAN port 12
LAN port LEDs
  described 13
  troubleshooting 199
Layer 2 subnet, access point autodiscovery 92
Layer 3 access point autodiscovery 91, 96
LDAP server 79, 86–88, 114
LEDs
  front panel 11
  startup procedure 39
  troubleshooting 198
legacy 802.1x authentication 78
levels, logging 59
licenses
  managing 165–167

number and types required 18
registering 54–57
load balancing 147
load balancing logs, viewing and saving 164
local access points 91, 98, 101
location, placement wireless controller 45
logs
configuring 58
viewing and saving 159

M

MAC authentication 81
MAC authentication groups 84
managed AP list 100
managed status, access points 101
management users, adding 116
management VLANs 23, 27, 49
maximum burst length 146
maximum number, wireless clients 147
memory partition 155
minimum and maximum contention window (CwMin or CwMax) 146
models, access points supported 15
multicast, firmware upgrade process 168

N

neighboring clients, viewing 184
network authentication 69, 75
network performance, troubleshooting 203
notification server, emails 62
NTP (Network Time Protocol), client and server 48

O

option 43, DHCP 91

P

package contents 11
partition, memory 155
password requirements 207
passwords
restoring default 201
users 116
physical specifications 206
pinging, access points 203
planning, system 23
PoE (Power over Ethernet), access points 15
portals, configuring 111–115
ports and slots 11
Power LED
described 12
troubleshooting 198
power supplies 14
preamble type 131, 135
preventing channel allocation 139
product label 14
profile groups. *See*
access point profile groups.
advanced profile groups.
basic profile group.
profiles. *See* security profiles.

Q

QoS (quality of service) 144

R

rack-mounting 45
radio frequency (RF)
logs, viewing and saving 164
management 140
obstructions 23
radio, turning on and off 126
RADIUS authentication server groups 88
RADIUS servers 79, 85–87, 114
rate limit logs, viewing and saving 165
rate limiting 148
rebooting
access points 167
wireless controller 156, 201
received signal strength indication (RSSI) 148
reduced interframe space (RIFS) transmission 131, 135
registration keys, licenses 57, 166
regulatory compliance 207
remote access 157
remote access points 94, 98, 101
requirements Layer 3 autodiscovery 91
Reset button 12
resetting
factory defaults 12
passwords 201
wireless controller 156
restoring the configuration 153
RF (radio frequency)
logs, viewing and saving 164
management 140
obstructions 23
RIFS (reduced interframe space) transmission 131, 135
roadmaps for configuration 42–44

rogue access points
detecting and managing 108
viewing
on the managed access point 180, 192
on the wireless controller 174, 185
RSSI (received signal strength indication) 148
RTS threshold 130, 134

S

scheduling
channel allocation 139
firmware updates, wireless controller 155
radio 126
security profiles
configuring
advanced profile groups 73
basic profile group 67
managing 64
viewing on the access point 179, 192
viewing on the wireless controller 186
self-healing 142, 143
server, licenses 54
service set ID (SSID) 68, 74
session time-out 159
SFP slots and LEDs, described 12–13
shared key requirements (RADIUS) 207
signal strength 147
slots and ports 11
sniffer 200
SNMP, enabling 157
soft reset 156
software
minimum version for access points 15
multicast, using for access point upgrade 168
upgrading, wireless controller 153
spectrum analysis 23
SSID (service set ID or wireless network name) 68, 74
Stack Master LED, described 13
standalone mode, access points
autodiscovery 96
returning to 104
Status LED
described 12
troubleshooting 198
subnet masks
access point 103
DHCP server 52
wireless controller 50
support, NETGEAR 18
syslog server 60
system alerts, viewing and saving 163
system logs, viewing and saving 159
system planning 23

T

tagged VLANs 49
TCP/IP network, troubleshooting 200
technical specifications 206
technical support 2
temperatures, operating and storage 206
Temporal Key Integrity Protocol (TKIP) 79
TFTP server, firmware upgrade 154
time and time zone
configuring 48
troubleshooting 202
TKIP (Temporal Key Integrity Protocol) 79
tracing a route 204
tracing events 59
trademarks 2
transmission opportunity (TXOP) limit 147
transmission power
automatically controlling 141, 143
manually controlling 133, 137
overriding 131, 135
trap port, SNMP 158
troubleshooting
access points 202
basic functioning 198
configuration settings, using sniffer 200
connection problems 203
date 202
diagnostic tools 203
discovery problems 202
GUI 199
LAN path 200
LEDs 198
network performance 203
pinging access points 203
restoring factory default settings 201
TCP/IP network 200
time and time zone 202
tracing an access point route 204
web management interface 199
Tx power
automatically controlling 141, 143
manually controlling 133, 137
overriding 131, 135
TXOP (transmission opportunity) limit 147

U

unicast, firmware upgrade process 168
unknown rogue access points 110

untagged VLANs 49, 103
upgrading firmware, wireless controller 153
USB port 12
users, managing 116

V

VAR information, licenses 56
video QoS queue 144
VLANs 49
  clients 24, 27
  DHCP server 52
  management 23, 27
  security profiles 69, 75
  settings, access points 103
  untagged 49, 103
voice calls, preventing channel allocation 139
voice QoS queue 144

W

web management interface
  layout 41
  troubleshooting 199
weight, wireless controller 206
WEP encryption 78
WEP key requirements 207
WiFi clients, adding 118
WINS servers 50
wireless band usage, viewing 175
wireless client separation 69, 75
wireless clients, maximum number 147
wireless clients, viewing
  in the network 194
  neighboring in the network 184
  on the access point 179, 192
  on the wireless controller 174, 182
wireless controller, viewing
  active SSIDs 190
  captive portal accounts and users 188
  DHCP leases 187
  managed access points 176
  managed clients 180
  neighboring access points 185
  neighboring clients 184
  profiles 186
  summary 173
  usage 175
wireless modes 130, 134
wireless network name (SSID) 68, 74
wireless settings 124
wizard, access point discovery 91
WLAN group assignment 104
WLAN healing 140
WMM (Wi-Fi multimedia) 144
WNAP210, WNAP320, WNDAP350, WNDAP360, and WNDAP380R 15
WPA and WPA2 authentication 79–80
WPA passphrase requirements 207